

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 7 August 1998		3. REPORT TYPE AND DATES COVERED
4. TITLE AND SUBTITLE THE EFFECTS OF TRUTH BIAS ON ARTIFACT-USER RELATIONSHIPS: AN INVESTIGATION OF FACTORS FOR IMPROVING DECEPTION DETECTION IN ARTIFACT PRODUCED INFORMATION			5. FUNDING NUMBERS	
6. AUTHOR(S) DAVID P. BIROS				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) THE FLORIDA STATE UNIVERSITY			8. PERFORMING ORGANIZATION REPORT NUMBER  98-019D	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) THE DEPARTMENT OF THE AIR FORCE AFIT/CIA, BLDG 125 2950 P STREET WPAFB OH 45433			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION AVAILABILITY STATEMENT Unlimited distribution In Accordance With 35-205/AFIT Sup 1			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words)				
14. SUBJECT TERMS			15. NUMBER OF PAGES 188	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT		18. SECURITY CLASSIFICATION OF THIS PAGE		19. SECURITY CLASSIFICATION OF ABSTRACT
20. LIMITATION OF ABSTRACT				

PII Redacted

Standard Form 298 (Rev. 2-89) (EG)  
Prescribed by ANSI Std. Z39.18  
Designed using Perform Pro, WWS/DIOR, Oct 84

THE EFFECTS OF TRUTH BIAS ON ARTIFACT-USER RELATIONSHIPS:  
AN INVESTIGATION OF FACTORS FOR IMPROVING DECEPTION  
DETECTION IN ARTIFACT PRODUCED INFORMATION

Name: David P. Biros  
Department: Information and Management Sciences  
Major Professor: Dr. Joey F. George  
Degree: Doctor of Philosophy  
Term Degree Awarded: Summer 1998

A number of studies have been accomplished examining the 'truth bias' individuals have toward others with whom they have a close relationship or familiarity (McCornack and Parks, 1986; Levine and McCornack, 1992; Stiff, Kim and Ramesh, 1992). However, little has been done to examine the relationship between individuals and information artifacts. Does truth bias affect an individual's ability to detection strategic information manipulation in artifact-produced information? Are there measures that can be taken to improve the deception detection capabilities of artifact users? This research examines the artifact user relationship and proposes a research model depicting the competing nature of artifact truth bias and detection factors such as experience, arousal and training as they influence an individual's ability to detect deception in artifact-produced information. The model was empirically tested in a laboratory experiment that included the use of a survey instrument. Together, the information collecting methods are used to gain a better understanding of the factors involved in strategic information manipulation and deception detection via artifacts.

DTIC QUALITY INSPECTED 1

19980811 121

THE EFFECTS OF TRUTH BIAS ON ARTIFACT-USER RELATIONSHIPS:  
AN INVESTIGATION OF FACTORS FOR IMPROVING DECEPTION  
DETECTION IN ARTIFACT PRODUCED INFORMATION

Name: David P. Biros  
Department: Information and Management Sciences  
Major Professor: Dr. Joey F. George  
Degree: Doctor of Philosophy  
Term Degree Awarded: Summer 1998

A number of studies have been accomplished examining the 'truth bias' individuals have toward others with whom they have a close relationship or familiarity (McCornack and Parks, 1986; Levine and McCornack, 1992; Stiff, Kim and Ramesh, 1992). However, little has been done to examine the relationship between individuals and information artifacts. Does truth bias affect an individual's ability to detect strategic information manipulation in artifact-produced information? Are there measures that can be taken to improve the deception detection capabilities of artifact users? This research examines the artifact user relationship and proposes a research model depicting the competing nature of artifact truth bias and detection factors such as experience, arousal and training as they influence an individual's ability to detect deception in artifact-produced information. The model was empirically tested in a laboratory experiment that included the use of a survey instrument. Together, the information collecting methods are used to gain a better understanding of the factors involved in strategic information manipulation and deception detection via artifacts.

THE FLORIDA STATE UNIVERSITY

COLLEGE OF BUSINESS

**THE EFFECTS OF TRUTH BIAS ON ARTIFACT-USER RELATIONSHIPS:**

**AN INVESTIGATION OF FACTORS FOR IMPROVING DECEPTION**

**DETECTION IN ARTIFACT PRODUCED INFORMATION**

By

DAVID P. BIROS

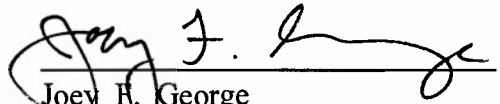
A Dissertation Submitted to the  
Department of Information and Management Sciences  
in partial fulfillment of the  
requirements for the degree of  
Doctor of Philosophy

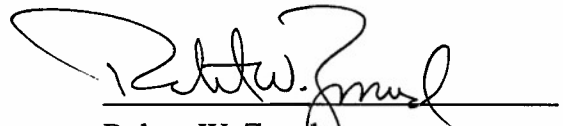
Degree Awarded:  
Summer Semester, 1998

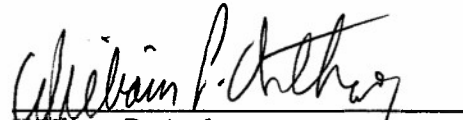
Copyright © 1998  
David P. Biros  
All Rights Reserved



The members of the Committee approve the dissertation of David P. Biros  
defended on June 11, 1998.

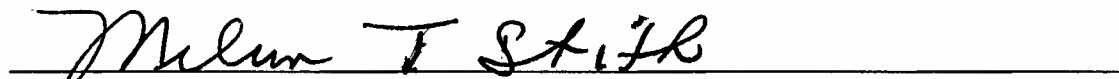
  
Joey R. George  
Professor Co-Directing Dissertation

  
Robert W. Zmud  
Professor Co-Directing Dissertation

  
William P. Anthony  
Outside Committee Member

  
V. Sambamurthy  
Committee Member

Approved:

  
Melvin T. Stith, Dean, College of Business

Dedicated to Pam, Jacob, and Joshua whose love and friendship are gratefully appreciated.

## ACKNOWLEDGEMENTS

I have come to learn that producing a dissertation is an education in itself. There are several people I would like to thank for their time and assistance in this process.

First, I would like to thank all of the members of my dissertation committee for their invaluable comments and guidance throughout the process. I would especially like to thank my co-chairs, Professors Joey George and Bob Zmud for their comments, suggestions, and wisdom. This word of thanks is not only for their support of this dissertation, but for the many lessons they taught me throughout my PhD program.

I would also like to express my appreciation to my wife, Pam, who kept the home fires burning throughout this process. You have supported me through three degree programs, endured my numerous data collection trips, and put your own aspirations on hold to further my success. I cannot thank you enough. I truly got the best end of the bargain when I married you!

Finally, I would like to thank my boys, Jake and Josh, for believing that their dad can do just about anything. You guys can brighten my day with just a smile and hug. One day, you will realize just how important that is.

## TABLE OF CONTENTS

LIST OF TABLES	viii
LIST OF FIGURES	ix
ABSTRACT	x
INTRODUCTION	1
LITERATURE REVIEW	7
Theories of Information Manipulation and Deception	8
Truth Bias	9
Information Manipulation Theory	10
Quantity	10
Quality	10
Relation	10
Manner	11
Interpersonal Deception Theory	12
The Need for Expanded Theory of Information Manipulation	13
Proliferation of Artifacts	14
Human Attitude Toward Computers	15
Human Trust in Artifacts	18
Computer-Based Protection from Manipulation	21
Human Ability to Detect Deception	23
Aroused Suspicion	24
Detecting Contextual Deception	25
Error Detection	26
Training for Deception	29
Summary and Conclusions	31
RESEARCH MODEL	33
Conceptual Model of Artifact/User Truth Bias Development	33
A Conceptualization of Deception Detection Methods	36
User Experience in the Domain	36
Arousal	37
Training for Deception Detection	38

Research Model of Truth Bias and Deception Detection Factors	41
Variable Descriptions, Hypothesis Development and Model Operationalization	42
METHODOLOGY	49
Proposed Site	49
The Information System	50
Study Design	52
The Experiment	52
The Matrix Design	55
Classroom Scenario	57
Data Manipulation	57
Control and Treatment Groups	61
The Attitude Scales	64
RESULTS AND ANALYSIS	68
Survey Findings	68
Group Size	69
Experience Level	72
Trust Toward PC-III	74
Analysis of Survey Instrument	77
Scale Reliability	78
Test of Hypotheses	80
The Effect of Truth Bias on Deception Detection Ability	80
The Effect of Experience on Deception Detection Ability	85
The Effect of Arousal on Deception Detection Ability	89
The Effect of Training on Deception Detection Ability	94
The Interaction Effect	96
Post Hoc Analysis	99
Discussion	101
CONCLUSION	108
Summary of Findings	109
Academic Implications	112
Management Implications	115
Strengths	118
Limitations	119
Opportunities for Future Research	121
Summary	123
APPENDIX A - Experiment Task Scenarios	124
APPENDIX B - Information Manipulation Descriptions	132

APPENDIX C - PC-III Screens	146
APPENDIX D - Discrepancy Reporting Sheet	162
APPENDIX E - Strategy of Manipulations	164
APPENDIX F - Deception Taxonomy Lesson Plan	168
APPENDIX G - Survey Instrument	172
APPENDIX H - Additional Scales	176
REFERENCES	180
BIOGRAPHICAL SKETCH	188

## LIST OF TABLES

<b>Table 2-1</b> Dimensions of Quality	28
<b>Table 2-2</b> Taxonomy of Deceptive Tactics	30
<b>Table 5-1</b> Summary Statistics of Survey Findings	69
<b>Table 5-2</b> ANOVA of Reported Truth Bias Levels Between Group Types	75
<b>Table 5-3</b> ANOVA of Reported Truth Bias Levels Between Treatment Groups	76
<b>Table 5-4</b> Alphas for Groups and Complete Sample	79
<b>Table 5-5</b> Mean Correct Hit Score By Truth Bias Level	82
<b>Table 5-6</b> Reliability Analysis of the Scales	84
<b>Table 5-7</b> Pearson Correlation of the Scales	84
<b>Table 5-8</b> Descriptive Statistics of All Scales	85
<b>Table 5-9</b> ANOVA of Experienced vs. Inexperienced User Deception Detection Performance	87
<b>Table 5-10</b> ANOVA of Craftsman vs. Officer vs. Apprentice Groups	88
<b>Table 5-11</b> ANOVA of Aroused Groups vs. Non-aroused Groups	90
<b>Table 5-12</b> ANOVA of Aroused-only Groups vs. Control Groups	91
<b>Table 5-13</b> ANOVA of Aroused-only vs. Control Group False Alarms	93
<b>Table 5-14</b> ANOVA of all Trained Groups vs. all Untrained Groups	95
<b>Table 5-15</b> ANOVA of all Groups	97
<b>Table 5-16</b> Mean Scores of Correct Detections for all Groups	97
<b>Table 5-17</b> Tukey's HSD of All Groups	98
<b>Table 5-18</b> ANOVA of Task Completion Rates of Aroused vs. Non-aroused	98
<b>Table 5-19</b> Summary of Findings	102

## LIST OF FIGURES

<b>Figure 2-1</b> Presence of Errors and Detector Responses	27
<b>Figure 3-1</b> Conceptual Model of Artifact Truth Bias Development	34
<b>Figure 3-2</b> Artifact Truth Bias and Deception Detection Ability Relationship	35
<b>Figure 3-3</b> IMT Based Taxonomy of Deceptive Practices	40
<b>Figure 3-4</b> Influences of Deception Detection Ability	42
<b>Figure 4-1</b> Field Experiment Model	56



## ABSTRACT

A number of studies have been accomplished examining the 'truth bias' individuals have toward others with whom they have a close relationship or familiarity (McCornack and Parks, 1986; Levine and McCornack, 1992; Stiff, Kim and Ramesh, 1992). However, little has been done to examine the relationship between individuals and information artifacts. Does truth bias affect an individual's ability to detect strategic information manipulation in artifact-produced information? Are there measures that can be taken to improve the deception detection capabilities of artifact users? This research examines the artifact-user relationship and proposes a research model depicting the competing nature of artifact truth bias and detection factors such as experience, arousal and training as they influence an individual's ability to detect deception in artifact-produced information. The model was empirically tested in a laboratory experiment that included the use of a survey instrument. Together, the information collecting methods are used to gain a better understanding of the factors involved in strategic information manipulation and deception detection via artifacts.

## **CHAPTER 1**

### **INTRODUCTION**

In the last decade, there has been explosive growth in the use of electronic communications to include electronic mail, the Internet, electronic data interchange (EDI), and many other forms of computer-based information systems (Schlack, 1992; Tolly, 1994; Zmud, 1988). All of these forms of communications systems can be classified as "advanced information technology" (DeSanctis and Poole, 1994, p. 125; Huber, 1991). Advanced information technologies (AIT) include artifacts such as electronic communications, executive information systems, group support systems and "other technologies that enable multi-party participation in organizational activities through sophisticated information management" (DeSanctis and Poole, 1994, p. 121). Further, it has been reported that organizations intend to increase their use of AIT in the near future. (Mohan, 1995; Day, 1995; Kornel, 1989; Sullivan, 1995).

As use of AIT grows, individuals and organizations come to depend on these systems for their decision making needs. In many cases, people come to trust the information systems they use to provide correct information (Wiener, 1985; Parasuraman, 1987). When this occurs, information system users make themselves vulnerable to errors in the data used by the information system and conditions of "strategic information

manipulation" (Zmud, 1990). They become susceptible to attacks on their information systems by those wanting to influence their decision making behaviors. Thus, errors in data and strategic information manipulation are two significant conditions faced by those who depend on information systems for their decision making needs.

The realm of data error has a long history of research that cross various fields of study. These include areas of vigilance (Davies, 1969; Weiner, 1987; Adams, 1987), attention (Parasuraman, 1984); and human ability to detect errors in data (Klein, et al., 1997; Klein, 1997; Johnson, et al., 1993). On the other hand, very little is known about strategic information manipulation. While there have been some studies and references to computer crimes and information manipulation toward the goal of embezzlement, very little has been accomplished with regard to influence on decision making (Johnson, et al., 1993; Bequai, 1987; Mungo and Clough, 1992; Shimomura, 1996).

In recent years, the United States military and the civilian sector have noted concern regarding the dangers of strategic information manipulation. In the mid-1980s, the military launched an all out campaign to begin to prepare its troops for what it calls 'Information Warfare' (IW) or 'Information Age Warfare' (Fowler and Peterson, 1997; Goodman, 1996, Libiki, 1995). The United State Air Force defines information warfare as "...any action to deny, exploit, corrupt, or destroy the enemy's information and information functions; protecting ourselves against those actions; and exploiting our own military information functions" (USAF IW pamphlet, 1996). Thus, the 'infosphere' joins air, land, sea, and space, as a potential battleground. The Air Force views IW as an

offensive and defensive operation. The prevention and detection of strategic information manipulation would be considered a defensive operation, or as named by the Air Force, 'counter-information operations.'

The concern regarding information warfare extends to the civilian sector as well. This can be attributed to two factors. First, civilian organizations are often closely linked to military organizations. Several military functions such as base security, network management, and database management either are currently, or will be, outsourced to civilian contractors in the near future. Further, the military conducts business electronically with hundreds of civilian business partners. Because of its need for information, the military cannot shut itself off from the civilian sector. Thus, civilian organizations can be seen as a possible weak link in the information security chain. Second, civilian organizations, in and of themselves, are vulnerable to information attacks (Malik, 1996, Mungo and Clough, 1992). While they may not face a military adversary, they may be subject to attacks from extortionists and unscrupulous competitors (Ibid.)

Studies and reports on computer and information security take a myopic view toward protection and system security. It appears the answers to all security problems are firewalls, encryption and other computer-oriented detection devices (Cobb, 1995; Moddy, 1995). Further, the Air Force Information Warfare Center (IWC) recently tested the safeguards used by network operators in the Air Force. Of the networks tested in the first on-line survey, 46 percent were successfully accessed, and IWC operators were able to obtain total control of 28 percent of the systems. In contrast, only 13 percent of all

systems tested reported any such break-in attempts or successes. The IWC operators found ways to circumvent the computer-oriented methods for system intrusion prevention and detection. This research highlights the importance of artifact users in the struggle for information security. When computer-oriented security measures fail, users should be seen as another line of defense. If users also have vulnerabilities, they must be identified and examined. This research endeavor synthesizes literature on individuals' ability to detect deception, truth bias, proliferation of information artifacts, and current trends toward information systems security in order to further understanding of the vulnerability of AIT users.

To date, little is known about the susceptibility of AIT users to forces that deliberately alter data in information systems in an effort to influence decision making behaviors. Do decision makers trust the AIT that is used to generate the information they need to make decisions? What types of users are most affected by the information manipulation? Can deceptive information be detected? Further, can arousal to the possibility of a manipulation and training of users to understand potential vulnerabilities improve detection results? The study that follows attempts to examine the questions by subjecting users of AIT to conditions whereby the information in the system they use on a daily basis is deliberately manipulated so as to influence their decision making behaviors. The research model for this experiment is founded on the construct of truth bias (McCornack and Parks, 1986). Truth bias occurs as individuals form relationships with others. Over time, as people communicate and build relationships with others, they

develop heuristics regarding the reliability of each of their acquaintances. As they begin to accept that they can believe what others are saying, they establish a truth bias. Thus, they become vulnerable to information manipulation (McCornack and Parks, 1986; Levine and McCornack, 1992; Stiff, Kim and Ramesh, 1992). Based on the truth bias construct and a review of existing literature, a conceptual framework is developed for understanding how people may be vulnerable to manipulation by information artifacts as well. From the conceptual framework, a research model and a series of hypotheses have been developed to explain the susceptibility of AIT user to strategic information manipulation and to identify possible countermeasures that may be taken to prevent such problems. The model and propositions are used to extend existing theory and examine the two following research questions:

- 1. Does truth bias influence an individual's perception of artifact reliability in the same manner it influences perceptions of human truthfulness?**
- 2. Can measures such as arousal and training be used to reduce human susceptibility to strategic information manipulation via information artifacts?**

The following chapters provide the background and conceptual framework for understanding truth bias and strategic information manipulation. Chapter Two reviews and synthesizes the literature on truth bias, deceptive communications, error detection, and artifact use and dependence. In Chapter Three, a research model is developed depicting the relationship of truth bias to an individual's potential for deception and the effects of arousal and training as means to reduce deception. Chapter Four outlines a lab experiment designed to test the research model and hypotheses in a real-world setting. A

description of the location and subject-task characteristics is included to further clarify the endeavor.

## **CHAPTER 2**

### **LITERATURE REVIEW**

Information manipulation and deception, in and of themselves, are complex phenomena that draw interest from many different fields of study. However, as Zmud (1990) noted, new information technologies have the potential to impact the perpetration of strategic information behaviors in rather unique ways. Individuals do misrepresent or restrict information in order to influence the behaviors of others (Feldman and March, 1981; Miller and Stiff, 1993, Johnson et al, 1993). The addition of advanced information technologies to the phenomena of information manipulation and deception adds to their complexity.

The purposes of this chapter are twofold. First, this chapter will review the relevant literature and provide a synthesized framework with which to continue the investigation into this emerging phenomenon of strategic information manipulation through artifact channels. Second, this chapter will establish the scope of the study. The first section reviews some of the theoretical bases for information manipulation and deception to include the truth bias construct (McCornack and Parks, 1986), information manipulation theory (McCornack, 1992), and interpersonal deception theory (Buller and Burgoon, 1996a). The second section examines the need for expanding such person-to-



person theories of communication to conditions whereby humans interact with artifacts for their information needs. This section will examine the proliferation of information artifacts, human attitude toward IT, and current computer-based protection mechanisms against strategic information manipulation. The third section examines human ability to detect deception and includes background information on attention and vigilance, error detection, and signal detection theory. It also reviews a taxonomy of deceptive practices that may help to create a viable detection training program. The final section summarizes and critiques the literature. A void in the current literature is identified and a suggested area of study is offered to help resolve this weakness in the understanding of strategic information manipulation and deception.

### **Theories of Information Manipulation and Deception**

The theoretical background regarding information manipulation and deception between human senders and receivers is rich and has been supported by some empirical testing (McCornack and Parks, 1986; Buller and Burgoon, 1993; McCornack and Levine, 1990; Levine and McCornack, 1991; Burgoon, Buller, Ebesu, and Rockwell, 1994). Such theories extend the body of knowledge about deceptive communications between sender and receiver. Three complementary theories of deception will be reviewed in this section: truth bias, information manipulation theory, and interpersonal deception theory.

## **Truth Bias**

McCornack and Parks (1986) introduce the concept of 'truth bias' as a reason why people have difficulty in detecting deception from familiar human sources. People develop relationships with others. Over time, they come to believe that what is told to them by a trusted partner is the truth. Of course, relationships whereby the receiver believes the sender's information cannot be trusted can occur as well. However, the focus of truth bias is that of a trusting relationship. Eventually, receivers incorporate heuristics to evaluate the reliability of the source (Tversky and Kahneman, 1974). For instance, if a receiver develops a close relationship with the sender, over time the former begins to trust the latter. The receiver develops a heuristic of trust toward that particular sender. Since the sender was reliable in the past, the receiver believes all communication will be reliable in the future. Thus, a truth bias is formed. Levine and McCornack (1992) empirically tested the truth bias model and found that it held. However, other tests (see Buller, 1988 and Stiff et al., 1992), labeled "pseudo-replications" by Levine and McCornack (1992, p. 152), found evidence to the contrary. Further investigation of the truth bias construct is warranted.

The construct of truth bias has been used in many conceptual and empirical studies of information deception and detection (Buller and Burgoon, 1994; Stiff, et al. 1992; Buller, 1988; McCornack 1992; McCornack et al., 1992). It has become a cornerstone of information manipulation and deception theory. Two key theories that provide additional understanding of this phenomenon are McCornack's Information

Manipulation Theory (1992) and Buller and Burgoon's Interpersonal Deception Theory (1996). Both theories are reviewed below.

### **Information Manipulation Theory**

This theory is an adaptation to the Cooperative Principle (Grice, 1989) in that it applies the cooperative maxims introduced in that research to communication principles. According to McCornack, "Messages that are commonly thought of as deceptive derive from covert violations of the conversational maxims" (1992, p. 5). Information Manipulation Theory highlights four maxims of communication that, when violated, can be considered a deviation from rational and cooperative behavior. The four maxims are as follows:

**Quantity.** This relates to the amount of information that should be provided in the message. The amount of information presented should be only as much as required for the situation. Purposeful addition of non-required information or deletion of necessary information is considered a violation of the maxim.

**Quality.** This relates to the veracity of the information. "Participants are expected not to present information they know to be false, nor make claims for which they lack adequate evidence" (Ibid., p.5). Knowingly falsifying information violates this maxim.

**Relation.** Violations of the relation maxim divert the communication from a danger of disclosure to a different subject. In layman's terms, this maxim might be best described as 'avoiding the subject.'

**Manner.** This refers to the way in which the information is presented. Often this form of manipulation transforms the communication into a rather ambiguous transfer of information. For instance, as a student constructs a research paper, a colleague might ask 'How far along are you?' His answer might be 'I'm on chapter four.' However, if he did not want to disclose how much or how little he accomplished, he might say, 'Oh, I am moving right along.' The second answer is not a lie, but it is very ambiguous.

Violating one or more of these maxims is a form of deception in communication. "IMT argues that one way of thinking about how deceptive messages become 'deceptive' is in terms of how the information that interactants possess is manipulated within the messages that they produce" (Ibid., p. 13). The key focus of IMT is the communication process. Empirical testing, while limited, has shown support for the theory (McCornack, Levine, Solowczuk, Torres, and Campbell, 1992). However, a more recent study by Jacobs, Dawson, and Brashers (1996) that replicated McCornack, et al. (1992) suggest that deception arises only for *quality implicatures* or inferences by the receiver made about the quality of information from the sender. In short, "...deceptions occur by inviting false implicatures" (Jacobs, et al., p. 71). Consideration of the other three maxims is unnecessary. In a critical rejoinder, McCornack, Levine, Solowczuk, Torres, and Campbell (1996) reanalyze the data and demonstrate how the data is inconsistent with the premise that deception arises only from such implicatures.

## **Interpersonal Deception Theory**

Buller and Burgoon (1996) offer Interpersonal Deception Theory (IDT) as a framework for understanding and explaining the dynamics of deception during interpersonal interaction. IDT posits that "a major factor in deception is one's communication skills" (Burgoon, Buller, and Guerreo, 1995, p. 290). In order to achieve successful deception, deceivers must demonstrate several verbal and nonverbal skills simultaneously. "They must plan and encode credible verbal messages while projecting a believable nonverbal image..." (Ibid.).

Interpersonal Deception Theory differs from IMT in that it focuses on face-to-face encounters. This is in contrast to Information Manipulation Theory where the focus is on the communication interaction and is more contextual in nature. Further, IDT delineates five fundamental dimensions including completeness, veracity, directness/relevance, clarity, and personalization as alternatives to the four maxims of IMT (Burgoon, Buller, Guerreo, Afifi, and Feldman, 1996). However, the theories are closely related. First, both emphasize the familiarity between sender and receiver. Burgoon and Buller suggest that this is somewhat novel as "most deception research has employed deceivers and detectors who are strangers to one another and therefore may not be relevant to ordinary deceptive encounters" (1994, p. 158). Second, since familiarity is implied in both theories, truth bias is a key construct. Finally, if suspicion is aroused as to the veracity of the transactions, the receiver's awareness will enable him or her to set up some form of defensive posture such as deception bias.

Like McCornack's theory, IDT has also received empirical support (Burgoon, et al., 1995; Burgoon and Buller, 1994). However, much of the support for IDT involves the receiver's ability to notice nonverbal cues as a means of detecting deception. Interpersonal Deception Theory, and to a lesser extent IMT, assumes communication is a phenomenon that only takes place between two human interactants. Recently, McCornack et al., (1996) have suggested that IDT's conceptual definitions lack precision and it does not contribute to the knowledge of deception. In a rejoinder to that critique, Buller and Burgoon (1996) maintain that IDT has empirical support and suggest IMT does not. However, a review of the literature suggests that the only empirical support for either of the theories is derived from experiments by those who conceptualized them.

In the past two decades, more and more communication is taking place not face-to-face but via artifact channels that are provided by advanced information technologies (Zmud, 1990). It is because of this growth in AIT that these theories need to be expanded to include human-to-artifact relationships. The following section discusses the reasons behind a need for expanded theoretical support of information manipulation in human-to-artifact communication.

### **The Need for Expanded Theory of Information Manipulation**

Advanced information technology has seen remarkable growth in the recent past, and it is projected to continue expanding in the near future (Schlack, 1992; Mohan,

1995). As such, much of the communication that takes place will be via channels such as electronic mail and the Internet. Zmud labeled these channels *artifacts* which he defines as..."computer- and communication-based information systems..." (1990, p. 97). Further, he posits that: 1) people will become increasingly dependent on artifacts as information sources, 2) they will place increasing confidence in information obtained from artifacts, 3) manipulative behavior will increasingly occur via artifacts, and 4) the perpetrators of deceptive behavior will be increasingly difficult to identify (Zmud, 1990).

A key notion implied through this work is that information manipulation can extend beyond person-to-person interactions and exist in person-to-artifact relationships. Based on this notion, the proliferation of artifacts, human attitude toward such artifacts, and their vulnerability to attack or manipulation by the human actors that utilize them will be considered in more detail.

### **Proliferation of Information Artifacts**

Advanced information technologies are widespread in organizations and continue to grow. Countless articles and studies in both the academic and popular literature report AIT's continued growth in organizations (Day, 1995; Hamilton, 1989; Jackson, 1995; Kornel, 1989; Schlack, 1992; Sullivan, 1995). These artifacts have become organizational tools that users have grown to depend on for their daily activities.

The proliferation of artifacts is projected to continue well beyond the year 2000 (Kornel, 1989). Not only is continued growth a factor, but evidence also suggests people prefer electronic forms of communication (Sullivan, 1995). Further, Davis (1989)

maintains that as individuals find technology to be useful they, will be apt to employ it. Also, O'Reilly (1982) found that information users appear to prefer accessibility to information more than they prefer accuracy. As the use of AIT continues to grow, it will influence the accessibility of information. First, often the employment of AIT replaces other channels of information accessibility, thereby making the new method more accessible. Second, the employment of AIT often brings information accessibility to users' desktops (where it may not have existed before), again, increasing accessibility to information. These reports and studies and their implications provide support for Zmud's propositions, noted earlier, as well as support for the argument to extend information manipulation theory. This suggests that protection from AIT-based information manipulation should be of concern.

While the proliferation of information artifacts in organizations is clear, it does not fully explain the artifact-human relationship. Artifacts may well populate the work place, but an understanding of human attitude toward the artifacts is a requisite for any study of strategic information manipulation via artifact channels and its detection. Fortunately, the existing body of literature on human attitude toward computers is quite rich. The following section will examine some of that literature.

### **Human Attitude Toward Computers**

Probably one of the most cited works on human attitude toward computers is the study by Davis, et al., (1989) that introduced the technology acceptance model (TAM). The model is based on the theory of reasoned action (Ajzen and Fishbein, 1980), which



suggests that a person engages in a specific behavior when he or she has the behavioral intention to perform the behavior. Behavioral intentions are based on the individual's attitude toward the behavior and the subjective norms regarding the behavior. In terms of computer usage, an individual's attitude or judgment that behavior is positive or negative plays a major role in their use of computers. Subjective norms concern the "...social pressures put on him to perform or not perform the behavior in question" (Ibid., p. 6). Thus, individuals will use computers in their work lives and daily lives when they believe it to be a positive behavior and/or when they believe others think that they should. In the work-place, subjective norms might be more of a driving factor when an individual's attitude toward usage is low. Davis, et al., (1989) introduced the TAM as an adaptation of the theory of reasoned action to as means of modeling user acceptance of information systems. They posited that perceived usefulness and perceived ease of use were of relevance to the acceptance of computer by users. In empirical testing, they found that perceived usefulness "...is a major determinant in people's intention to use computers" (Davis, et al., 1989, p. 997). However, there is much more to human attitude toward computers than intent to use.

In the late 1980's, a number of studies examined human attitude toward computers (Davis, 1989; Brown, et al., 1988; Popovich, et al., 1987; Koslowsky, et al., 1988). Morrison (1983) reported that although computers have been in use for quite some time, there was still a lack of positive acceptance by users and those affected by the technology. However, later studies resulted in conflicting findings. One key

component of positive attitude toward computer usage is time spent with the artifact. Popovich, et al., (1987) found in developing the Attitudes-Toward-Computer Usage Scale (ATCUS) that as participants in their study spent more time using computers, they "...showed a less negative reaction to computers and computer related technology..." (p. 266). Similarly, Davis (1989) and Brown, et al., (1988) found that increased exposure to computers and computer related devices appear to determine one's attitude toward the artifacts. Users with greater exposure have less negative attitudes.

Another key factor regarding positive (or, at least, non-negative) attitudes toward computers is the amount of training a person has related to computers. Popovich, et al., (1987) found that the more computer courses a person completes, the more positive that person's attitude toward computers. In a reexamination of the ATCUS, Brown, et al., (1988) derived similar findings. As such, individuals with computer education will more likely have a positive attitude than those with less education.

A final finding, and one that is somewhat more related to the study at hand, concerns computer usage in the work place. Popovich, et al., (1987) found in their study that males generally had a more positive attitude than females, and younger people had a more positive attitude (toward computers) than older people. However, when computers were required as tools for completing tasks in the work place, differences in attitude were quite reduced. Morrison (1983) reported similar findings in his survey of attitudes toward computers.

In summary, the literature suggests that amount of exposure to computers, the amount of computer training, and the level of work, related to computer use, all have an influence on computer attitude. Of course, some of these finding may be related. An individual who uses computers in the work place is likely to be more exposed to computers than one who does not use computers as a tool. The point is that individuals who have a greater exposure to computers generally have a more positive attitude or comfort level toward them. As this comfort level increases, do humans then display a greater trust in the reliability of the information they receive from these artifacts? The following section examines this notion of human trust in artifact-produced information.

### **Human Trust in Artifacts**

On a daily basis, humans trust artifacts with a large portion of their information needs. One only need visit a grocery store or automatic teller machine to view that fact. Television news shows have reported on the consumers' dependence on the use of bar code scanners in grocery stores and the lack of checking by consumers to ensure they purchased the product at the correct price (e.g., NBC's Dateline, 16 Dec 97). Likewise, the academic literature has examined this phenomenon of human trust in artifact-produced information (Weiner, 1985; Schlegel 1986; Bequai, 1987; Parasuranam, 1987).

Much of the work on human trust in artifact-produced information comes by way of the field of aviation. Wiener (1985) discusses the implications of using cockpit automation and its affect on aircrews. He reports that cockpits were automated due to the:

increased speed and capabilities of jet aircraft, the explosive growth of air traffic, the complexity of the regulatory environment, the unbearable costs of an accident, and the recognition of human limitations (Wiener, 1985, p.77)

There are various reasons for automating the work environment, including economy, reliability and availability of information systems. As such, various information technologies have become necessary for many industries. Parasuraman (1987) describes a computerized monitoring device that air traffic controllers have come to rely on to assist them in their duties. The FBI and many municipal court systems rely on advanced information technology for the storage and maintenance of criminal records (Bequai, 1987). Further, many Federal agencies are currently reviewing electronic record keeping systems (ERKs) that can monitor information from creation to destruction based on disposition and destruction algorithms. Vital records may soon be placed under the purview of AIT. Also, the Air Force IWC encourages network systems administrators to use auditing systems to monitor file usage by network users. The auditing systems are computer programs used to monitor file usage activity by users. Using sophisticated algorithms, the programs track and record file usage. When a file is used in a non-normal manner or when significant changes have been made to the file, the program flags the file for possible abuse.

What is the meaning of this trust in artifact-produced information and reliance on artifacts? A number of problems are recognized. First, individual users of the technology learn to become dependent on it. Wiener (1987, p. 87) explains that cock-pit

automation has "taken the crews out of the loop to the extent that they may be unable to perform the supervisory and monitoring duties that we relegate to them." By having a high level of dependence on AIT, users can become unable to perform their tasks without such automated assistance. Second, by reducing the monitory workload, automation may lead to complacency and boredom. Parasuraman (1987) suggests that the goal of automating systems may not necessarily be to reduce the workload but to optimize it. Finally, reliance on artifact-produced information may cause users to not question the information they do receive and thereby base decisions on what is perceived or understood. In short, because the information arrives via an artifact channel, people tend to be influenced by the style of how it is presented (Schlegel, 1986).

All of the points mentioned above suggest that people in many different occupations and walks of life can become dependent on artifacts to meet their information needs. While the loss of appropriate job skills is important, the scope of this research is to examine how users might prevent themselves from deception via artifact channels. As more and more information tasks are automated, the vulnerability to strategic information manipulation increases (Zmud, 1990). Therefore, it becomes important to identify ways to prevent such deceptions.

Currently, two basic approaches of protection exist with regard to detecting strategic information manipulation: computer-based defenses and user-based defenses. While it is logical that both methods should be used concurrently, often computer-based approaches receive primary consideration for deception detection activities. A review of

these approaches including some the methods used and their weaknesses is offered below.

### **Computer-Based Protection from Manipulation**

One of the concerns of interest to this research is the potential for deception or information manipulation that takes place via human-to-artifact interactions. This deception may be derived from unauthorized users or authorized users manipulating the information. Preventing unauthorized use of artifacts often falls into the category of systems security.

Recent reports have noted that computer- and communication-based information systems have come increasingly under attack (Wright, 1994; Anthes, 1996a; Anthes, 1996b). These attacks come in the form of unauthorized use or manipulation of information, destruction of information or system-critical files, and exposure to computer viruses. Attackers could be anyone from outside hackers to disgruntled employees. In turn, systems security personnel have resorted to sophisticated measures to prevent unwanted access. For instance, Cobb (1995) reports that 'firewalls' are popular tools for protecting networks from unauthorized access. These tools can take the form of screening routers or packet filters, which reject connection attempts from unauthorized addresses, or application gateways that enable more direct control of Internet services and users (Moody, 1995). Another protective technology that is growing in popularity is encryption. With this technology, information is coded by the originating systems and

decoded by the receiving system with the correct decoding key. If a receiver (intended or unattended) does not have the key, the information cannot be decoded.

Computer-based security measures have become commonplace in many organizations. However, they have not significantly reduced the vulnerability faced by organizations from information manipulation (Anthes, 1996a). There are a number of reasons for this lack of performance. First, many computer-based security measures are not 'foolproof.' For instance, while an information system may be protected by a firewall allowing only certain originating addresses entry, a deceiver could gain access to an authorized address not protected by a firewall and thus gain access to the intended system (e.g., a telnet application). Second, computer-based security measures such as passwords can be thwarted by network monitoring whereby those intending to deceive can obtain passwords and other data simply by 'listening' to a network (Anthes, 1994; Grier, 1997). Third, perpetrators can also "social engineer" pieces of computer security information (Shimomura, 1996). Social engineering is a tactic used by people who manipulate artifacts and artifact produced information by talking unsuspecting users and systems administrators out of valuable information. Kevin Mitnick, a man who achieved almost legendary status in computer hacking circles, often relied on low-tech social engineering methods to learn the information he needed to gain access to computer systems (Ibid.) Finally, computer-based security measures are often ignored (Mohan, 1995). Among other problems, individuals create passwords that can easily be guessed, leave their terminals for long periods of time while being logged-in, and allowing others to know

their passwords. In some cases, the security measures are sidelined by the necessity of users to have ready access to the information (Alexander, 1990). This, in turn, increases vulnerabilities to manipulation.

Computer-based security measures do provide some protection from unwanted manipulation or attack and remain a vital deterrent even though they can be circumvented. However, the vulnerability to information manipulation is a problem even the US Department of Defense cannot currently overcome. In 1995 alone, DoD computers were attacked some 250,000 times, and nearly two-thirds of the attacks were successful (Anthes, 1996b). These figures remained unchanged in 1996 (Grier, 1997). Commercial systems face the same vulnerabilities.

### **Human Ability to Detect Deception**

When computer-based protection fails, users become the last line of defense at detecting deception. Unfortunately, some studies have shown that human ability to detect deception, in certain situations, is no better than chance (DePaulo, Stone, and Lassiter, 1985; DePaulo and DePaulo, 1989; Maier and Thurber, 1968; Feeley and de Turck, 1995). This lack of positive support of human detection of deception might suggest that people are not a feasible line of defense, however, two areas particularly of concern to human-to-artifact interrelations that show promise are cases of aroused suspicion and the use of contextual cues as a means of detecting deception.



## **Aroused Suspicion**

While in a state of normal interaction with other humans, people have trouble detecting deception. However, if for some reason suspicion is aroused, their ability to detect deception goes up (Parasuraman, 1984; Stiff, Kim, and Ramesh, 1992; Miller and Stiff, 1993). That is, if a receiver is forewarned that an incoming piece of information may have been manipulated, he or she is better able to detect the deception. In a sense, the arousal places the receiver at a 'state of alert.' As Stiff, et al., noted, "...suspicion aroused by a third party is an important part of veracity judgment" (1992, p. 342).

One note of importance is that aroused suspicion can also lead to increases in detection yet be unrelated to accuracy (Parasuraman, 1984; Toris and Depaulo, 1985). That is, while detection is improved, the rate of false alarms also increases. However, this may not be important given the current state of affairs regarding information systems security. If it is desirable to detect possible information manipulation or deceptive communications in AIT, then the cost of a few false alarms may be worth the effort. Thus, aroused suspicion may increase false alarms, but that may be a worthwhile cost if detection of truly deceptive practices can be increased.

One seeming disadvantage to detection deception in artifact-to-human relationships is the absence of physical gestures that may aid the receiver in detecting falsifications by the sender. In artifact-to-human communication, the actual sender of the information is not seen and the receiver must rely on the information and its context

for any signs of deception. The following section examines the literature on detecting deception without the aid of sender-receiver visual contact.

### **Detecting Contextual Deception**

The human-to-artifact relationship implies an absence of nonverbal cues for the receiver to use in detecting deception. While this may seem to be a disadvantage, research indicates that it may actually improve deception detection accuracy (Zuckerman, DePaulo, and Rosenthal, 1981; DePaulo, et al., 1985). In an earlier study, Maier and Thurber (1968) found that readers and listeners actually demonstrated a greater ability to judge dishonesty than watchers. That is, when receivers were able to see the nonverbal cues demonstrated by senders, they were less successful at detecting dishonesty than those who could only read the communication. The authors believe the visual cues supplied by the sender acted as distracters rather than helpful aids at detecting deception. Some senders actually learned to use the visual cues to their advantage. While this study is somewhat dated, more recent studies confirm the results. DePaulo, et al., (1985) and Zuckerman, et al., (1981) both found that detection accuracy was significantly more accurate when facial cues were not present than when they were available. These results provide promising support for the notion that contextual cues of the information can be used to accurately detect deception in communication. Similar findings have been identified in the area of error detection. The following section examines the relevant error detection literature and its relatedness to deception detection.

## Error Detection

Current research on error detection is quite plentiful, but rather undecided as to the ability of human to detect errors in computer outputs. Many of the studies on error detection use signal detection theory as a theoretical basis for understanding the phenomenon (Davies and Parasuraman, 1981). Signal detection theory has been applied to examine the accuracy and biases of internal auditors risk judgments (Blocher, et al., 1986), human attention (Sperling, 1984), and vigilance (Davies and Tune, (1969). Essentially, the theory is used for explaining the performance of humans distinguishing between two types of events: noise and signal. Noise can be thought of as background whereas a signal is a stimulus that differs from the background noise. In the context of deception detection, clean or untampered data might be considered noise and strategically manipulated data would provide a signal.

Much of the existing research suggests that humans are rather poor at detecting errors in information they receive from artifact channels (Laudon, 1986; Wiener, 1987; Rickets, 1990). However, recent studies conducted by Klein and her colleagues suggest that humans are better than previously thought with regard to error detection in computer derived information (Klein, 1996; Klein, et al., 1997a; Klein, et al., 1997b). There are two possible reasons for these differences. First, the earlier studies did not arouse respondents to the potential for data errors. Second, in many of the earlier studies, respondents were not made aware that capturing data errors was part of their task sets. In her most recent work, Klein suggests that there are four possible outcomes in error

detection tasks. These are presented in Figure 2-1 below. Not surprisingly, this depiction of the presence of errors and their detection is similar to the discussion of deception and detection presented earlier. That may be because both streams of research fall under a larger umbrella of data quality, an area, in and of itself, that is worthy of review.

		Behavior	
		Error Detected	Error Not Detected
Data	Error Exists	Hit	Miss
	Error Does Not Exist	False Alarm	Correct Rejection

**Figure 2-1- Presence of Errors and Detector Responses**

Although there exists no single definition of data or information quality, there has been a significant amount of research conducted in the area (Zmud, 1978; O'Reilly, 1982; Laudon, 1986; Svanks, 1988; Knight, 1992; Janson, 1988; Paradice and Fuerst, 1991). Zmud (1990) outlined four dimensions of information. Table 2-1, below exhibits those dimensions and their corresponding characteristics.

**Table 2-1 - Dimensions of Quality**

DMENSION	CHARACTERISTICS
QUANTITY	Complete, Sufficient
RELIABILITY	True, Reliable, Valid, Accurate
TIMELINESS	Current, Timely
FORMAT QUALITY	Readable, Orderly, Logical, Clear, Simple

Similarly, Huh, et al., (1990), identified four dimensions of quality: accuracy, completeness, consistency, and currency. Like the Klein, et al., (1997a) work in error detection, the scope of the current study is primarily concerned with data or information accuracy. As such, data or information accuracy will be defined as an agreement with an attribute of a real word entity, a value stored in another database (or source document, or the results of an arithmetic computation (Huh, et al., 1990)).

As in the case of error detection, detecting deceptive or strategically manipulated information suggests the detector is a person working with data or information that is derived from non-human sources such as artifacts like those defined earlier. The detector must identify the signal from either the information or the context in which the information is used without any nonverbal cues (e.g., gestures, expressions) from the sender of the information. The next question is then: Can individuals be trained to increase their deception detection abilities in artifact-to-human relationships? The following section will examine a recent study on fraud detection and suggest how it may be used in an effort to teach information users how to detect deceptive information.

## **Training for Deception Detection**

Deception detection is difficult in part due to the fact that most people have little experience with it. Studies on expertise suggest that those who are expert in a task tend to base their activities on patterns of information developed through experience (Claser and Chi, 1988; Larken, et al., 1980). Such patterns trigger solution methods that have been successful with similar problems in the past. That difficulty is also compounded by the fact that it is estimated between 1% and 10% of data items in organizational databases are inaccurate (Laudon, 1986; Klein, et al., 1997). Therefore, people who do believe they have detected deception may have simply detected a data error that was never meant to be a deception.

In their 1993 article on fraud detection in accounting, Johnson, et al., attempt to build strategies for constructing and detecting deception built on a taxonomy of tactics for cheating (Bowyer, 1982). Bowyer (1982) distinguishes two key strategies: dissimulation (hiding the real) and simulative (showing the false) deceptions. Johnson, et al., note that since the strategies are symmetrical, any tactic might be used for either strategic purpose. Table 2-2 outlines seven tactics for deception. Of those seven, six were established by Bowyer and the seventh, double play, was added by Johnson, et al., (1993). These tactics help to establish the type of activities a deceiver might use to manipulate information. Johnson, et al., (1993) believe that if the receiver or user of the

information can be made aware of these deceptive tactics, he or she can then learn to detect deception. They suggest that each of the deceptive tactics can be overcome by hypothesizing the event had occurred (if there is an expectation of its presence) and examining the data for the assumed tactic.

**Table 2-2 - Taxonomy of Deceptive Tactics**

<b>Tactic</b>	<b>Description</b>
Masking	Deleting from the environment attributes that suggest the correct representation.
Double Play	Manipulating attributes in the environment in a way so as to weakly suggest the correct representation. The purpose is to reinforce incorrect representations by weakly suggesting the correct one.
Mimicking	Modifying attributes in the environment in a way so as to suggest the incorrect representation. Essentially suggestions (not necessarily deceptions in and of themselves) are included to support the incorrect representation.
Dazzling	Modifying attributes in the environment in such a way as to obscure or blur those attributes whose interpretation suggests the correct representation and to emphasize those attributes whose interpretation suggests the incorrect one.
Inventing	Adding new attributes to the environment in order to suggest the incorrect representation.
Repackaging	Modifying attributes in the environment in order to hinder the generation of the correct representation. Repackaging is weaker than mimicking because it is based on justification and distortion rather than replication of attributes.
Decoying	Adds new attributes to the environment in order to hinder identification of the correct representation. It is weaker than inventing since the decoys are not directly suggestive of the incorrect one. It simply directs attention away from the correct one.

Of the three cases they described in their study, Johnson, et al., found that using "an intentional strategy may be a necessary but not sufficient condition to guarantee success" (1993, p. 485). They believe that one must understand the intentions of the

deceiving agent (i.e., arousal) and use strategies for detection in order thwart the seven deceptive tactics. The authors also point out that they have no theory on which to base their study and suggest that the taxonomy be used in areas other than accounting fraud in an attempt to gain greater understanding. Furthermore, it is the view of this author that such a method of deception detection should be tested on more than the performance of three respondents. In short, what is missing is adequate theory with which to sustain their taxonomy and suitable empirical testing in other venues.

### **Summary and Conclusions**

This chapter provided a review of the literature regarding theories of information manipulation, research of deception and deception detection, and work in related fields such as computer-based detection, user reliance on artifacts, information quality, error detection and fraud. The literature was used to outline the conceptual framework for the current study. Essentially, there are existing theories to explain the human-to-human phenomenon of information and deception. Truth bias is a key construct underlying these theories. However, the theories lack the ability to capture the phenomenon of artifact-to-human relationships.

Empirical research on deception and deception detection mostly examines the human-to-human relationship. Very little has been accomplished with artifacts. Related literature in the fields of computer acceptance and computer trust depicted today's



conditions as having a large proliferation of artifacts, increased dependence on artifacts for information needs, and inadequate protection from artifact-based information manipulation. What is missing from this research is an understanding of human ability to detect strategic information manipulation via advanced information technologies. This includes the influence of truth bias as a vulnerability to deception, arousal as a possible enhancer to detection in a computer mediated environment, and the plausibility of training artifact users to detect various types of deception in the artifact-produced information they use. Chapter Three will introduce the conceptualization of this situation and provide a research model to be applied in investigating the influence of truth bias on artifact/user relationships as well as factors that affect human ability to detection deception via information artifacts.

## **CHAPTER 3**

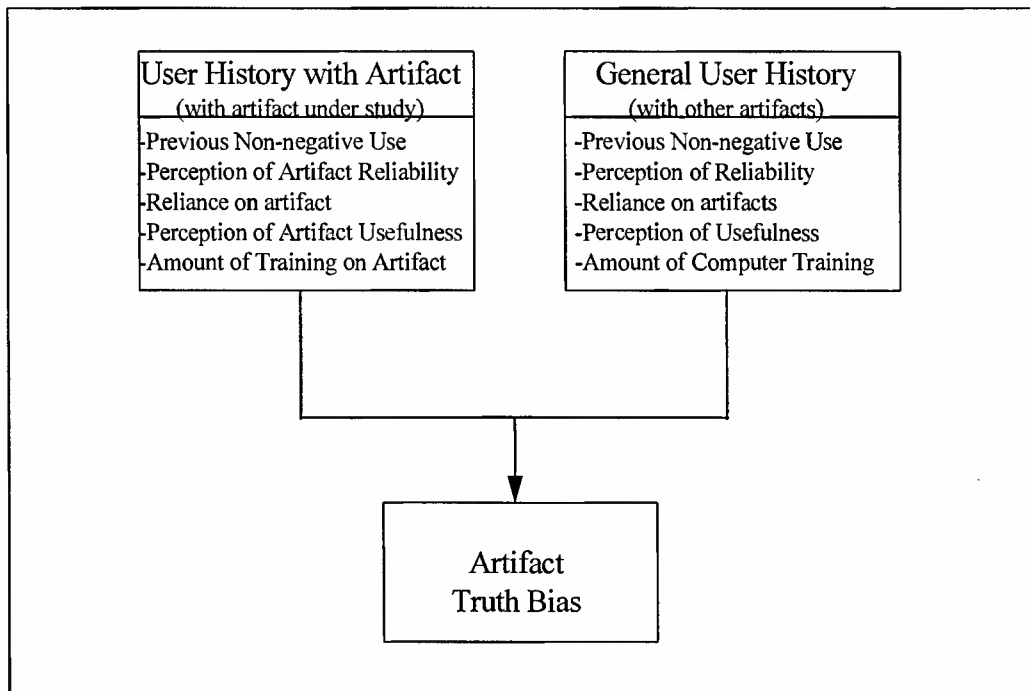
### **RESEARCH MODEL**

The existing theories of information and manipulation focus on human-to-human relationships. Truth bias is a construct essential to their explanation of the communications phenomenon of information manipulation. However, as noted, much of the communication that takes place today occurs via the use of artifacts. The numerous reports and studies outlined in Chapter 2 attest to that. Furthermore, over time, users begin to trust the artifacts from which they receive information. Opportunities for deceptive communications by computer- and communication-based information systems are indeed prevalent (Zmud, 1988). Yet no theory exists to adequately explain this. This chapter begins by conceptualizing the development of a user's truth bias toward an artifact.

#### **Conceptual Model of Artifact/User Truth Bias Development**

As a user begins a working relationship with the artifacts at his or her disposal, he or she brings a history of past experiences both with other artifacts and with people. This can include positive experiences with other artifacts, perceptions of reliability with

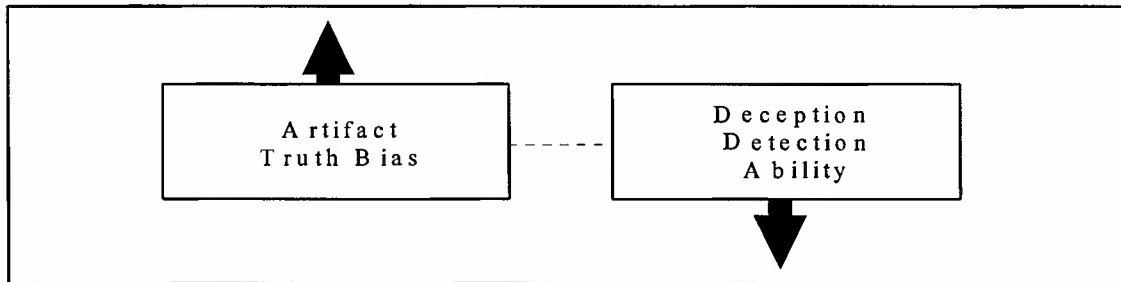
the artifact in use and other artifacts in general, a level of computer training, and other factors such as those depicted in Figure 3-1 below. As such, it is assumed that user history will affect the current artifact/user relationship.



**Figure 3-1 - Conceptual Model of Artifact Truth Bias Development**

As the human partner in the relationship begins to use the artifact, his or her heuristic of truth bias toward that artifact is developed and modified (McCornack and Parks, 1986). This, in turn, influences the user's perception of the artifact's reliability. When the user is comfortable with the artifact, he or she comes to rely on the artifact. This reliance will thus lead to the potential for deception. Thus, as the truth bias toward the artifact increases, an individual's vulnerability to strategic information manipulation

via the artifact increases and his or her ability to detection deception from the artifact should be reduced. This relationship is depicted in Figure 3-2.



**Figure 3-2 - Artifact Truth Bias and Deception Detection Ability Relationship**

The ability to detect deception in information provided through artifacts is reduced by a heuristic an individual uses to assess the reliability of the artifact in use. As the truth bias toward an artifact increases in strength, the individual's ability to detect deception is subsequently reduced due to the increased faith in the artifact. This is similar to a heuristic a person might use to assess the truthfulness of a human counterpart (McCornack and Parks, 1986). As noted, in the human-to-human relationship, the receiver is hindered in identifying instances of information manipulation by the sender. This, according to McCornack (1992), is due to the receiver making *implicatures* regarding the trustworthiness of the sender's message.

It is the purpose of this research to better understand the influence of truth bias on the human-artifact relationship. It is also the purpose of this research to examine factors that may help counter the influence on truth bias and its hindrance to deception detection.

The following section will examine some of these factors and outline their relationship to an individual's ability to detect deception in artifact produced information.

### **A Conceptualization of Deception Detection Methods**

Chapter 2 examined the literature on three general areas that have shown to improve error detection performance in artifact-produced data (Klein, 1996 and 1997a), fraud detection in artifact produced data (Johnson, et al., 1993), and deception detection performance in human-to-human relationships (Miller and Stiff, 1993, Burgoon, et al., 1994). These areas are experience of the receiver in the communication domain, arousal of the receiver to the possibility of deception, and training of the receiver to better detect when deception is occurring. While much of the research in these areas has been accomplished with regard to human-to-human communicative relationships, this research attempts to establish them as factors that may improve deception detection in artifact-to-human information relationships. Each of the areas will be discussed below.

#### **User Experience in the Domain**

Typically, users of a given domain of information appear to be better at detecting problems with the information if they have more experience in the domain. Johnson, et al. (1993) noted this in their study of accounting fraud detection. Klein, et al. (1997a) borrowed from Campbell's theory of task performance and suggest that knowledge and

experience may affect error detection performance by influencing an individual's ability to discriminate between correct and erroneous records (Campbell, 1990). In their study on MIS data quality, Paradice and Fuerst (1991) suggest that users perform error detection on an ad hoc basis when they observe peculiarities in the data, inferring that greater familiarization in the domain would lead to improved performance. Furthermore, a consideration of signal characteristics (Davies and Tune, 1969) would suggest that users with more knowledge and experience in the domain are better equipped to detect a wider set of signals from the background noise.

In summary, the literature on error detection, vigilance and signal detection suggests that greater experience in the information domain will lead to greater detection performance. Similarly, this current research project will posit that greater experience and knowledge in a given artifact domain will allow for better success at detecting deception. Along with experience, arousal of users to potential data problems should also increase detection performance. The next section will examine the nature of arousal on deception detection performance.

### **Arousal**

As noted in Chapter 2, arousal can have a positive effect on detection performance. It can also have a positive effect on false alarms (Parasuraman, 1984; Toris and Depaulo, 1985). In the case of deception detection, one must consider the importance of false alarms. Increasing deception detection performance involves increasing the user's *accuracy* of detection actual deceptions. Merely increasing the times

an individual sounds the alarm would be similar to the old fable of the boy who cried wolf. Early on, the alarms would be the cause of concern by those desiring to catch deceptions. However, too many false alarms might result in an air of complacency.

Another area of concern is task duration. Typically, an individual's ability to detect deception declines over time. This is especially true in a case where diligence tasks are long and monotonous (Davies and Tune, 1969; Miller and Stiff, 1993; Parasuraman, 1984). Parasuraman (1984) refers to this as *vigilance decrement* that, according to Wiener (1987), was first noted by Mackworth (1950). Increased arousal can help to reduce the level of vigilance decrement. However, prolonged task duration seems to have a negative influence on detection sensitivity even when arousal occurs. As such, the task duration must be considered a control variable in a vigilance related study such as this.

Thus, when an individual who has a truth bias toward an information artifact becomes aroused or suspicious of the reliability of the data produced by the artifact, deception detection should increase. However, even under conditions of arousal, as the length of the vigil task increases, the detection level should continue to decline. Thus, methods other than arousal (or used in combination with arousal) might be of value. One such option might be training the artifact user to understand and identify deception tactics as they might apply to their artifact domain. The next section considers such a training option.

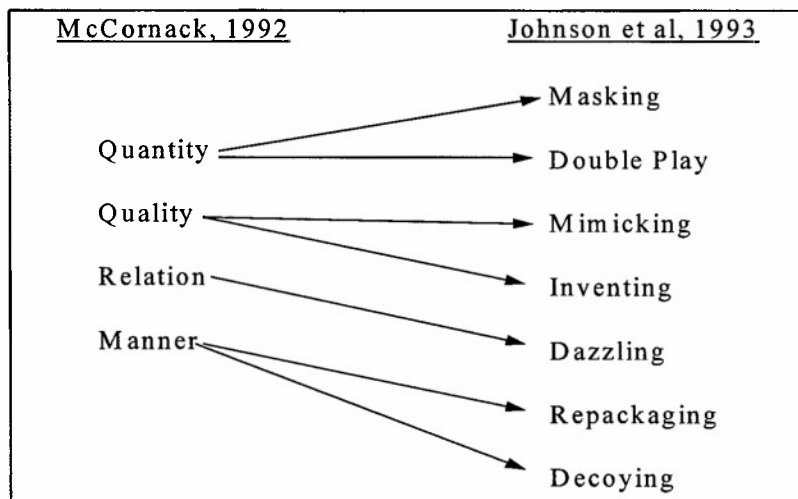
## **Training for Deception Detection**

Chapter Two highlighted a study by Johnson, et al. (1993) which used a taxonomy of tactics developed by Bowyer (1982) for constructing deception. In the study, Johnson and his colleagues adapted the seven tactics (see Table 2-2) to the field of accounting. They identified situations in an audit scenario whereby each of the deceptive tactics could be applied. Then, by training auditors to identify and understand the tactics, they appear to have improved their subjects' deception detection performances. Unfortunately, the study was limited in that only 3 auditors were used to examine the phenomenon. Furthermore, the authors had no theory on which to base their study. Interestingly, only a year prior in the field of communications, McCornack (1992) developed his Information Manipulation Theory (also noted in Chapter 2).

Under IMT, deceptive information or messages are derived from covert violations of four conversational maxims: quantity, quality, relation, and manner. A receiver or user of the information must make heuristic inferences or implicatures (from Grice's Cooperative Principle, 1969) regarding the trustworthiness of the sender or source of the information. As mentioned earlier, this inference making can lead to the creation of truth bias by the user toward the perceived source of the information. When that occurs, the potential for deception is increased. To date, IMT has enjoyed little empirical testing and has incurred some criticism regarding its conceptualization. Nonetheless, it may still prove to be useful for the current research project.



By combining the Johnson, et al. taxonomy (1993) and with McCornack's IMT (1992), it may be possible to theoretically ground the taxonomy and test theory in the current study of strategic information manipulation via artifact-produced information. In fact, the seven tactics in the taxonomy seem to factor nicely into the maxims of communication. Figure 3-3, below, depicts how such a union of the two might take place.



**Figure 3-3 - IMT Based Taxonomy of Deceptive Tactics**

Thus, while a deceptor may take advantage of a user's truth bias toward an artifact by violating the conversational maxims noted in IMT, there exist factors that may offset the negative influence of truth bias on the user's deception detection ability. These factors include: experience in the domain (i.e., information domain), arousal, and training for detection. With respect to Signal Detection Theory (Davies and Tune, 1969), increasing a user's ability to detect the signals of deception in information derived from

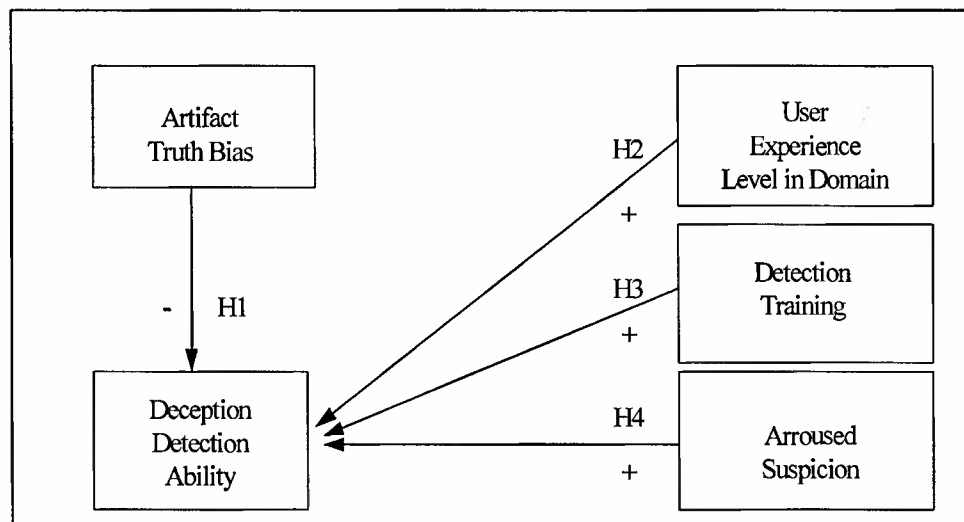
artifacts should produce increased performance in deception detection ability. This is similar to the theory of error detection proposed by Klein, et al. (1997). The difference being Klein and her colleagues were concerned with arousing and providing incentives to respondents to find errors. This research is aimed toward increasing the deception detection ability of artifact users by examining the three factors noted above.

With the theoretical foundation in place and factors that may improve deception detection identified, it is now possible to build a research model depicting the relationship of the detection improvement factors to truth bias and its influence on artifact user deception detection capability.

### **Research Model of Truth Bias and Deception Detection Factors**

This section will introduce a research model, define the necessary variables, and establish hypotheses to consider in order to study the influence of truth bias and related detection factors on artifact user deception detection abilities. The influence of truth bias on human-to-human communicative relationships has been documented and has been supported in some empirical testing. Similarly, factors such as respondent experience in the information domain, arousal, and detection training have all been introduced in the supporting literature. The following research model, illustrated in Figure 3-4, depicts the relationships of these constructs and their influence on the artifact/user deception detection capabilities.

The model depicts the competing nature of the various forces on an artifact user's deception detection ability. The following sub-sections will define the model's variables, introduce the hypotheses to be tested, and operationalize the relationships between variables in order to suggest methods for future testing.



**Figure 3-4 - Influences of Deception Detection Ability**

### **Variable Descriptions, Hypothesis Development and Model Operationalization**

The only dependent variable in the model is Deception Detection Ability. Since one of the objectives of this research is to improve artifact user deception detection abilities, this seems appropriate. Deception detection ability is defined as competence at correctly detecting deceptions (strategic information manipulations) in the information derived from the artifact in use. As in the case of error detection (See Figure 2-1),

deception detection ability is considered substantial when the level of "hits" and "correct rejections" is high and the level of "false alarms" and "misses" is low.

The independent variables are all factors influencing the users' deception detection ability. General User History and User History with Artifact act together to establish a user's Artifact Truth Bias (See Figure 3-1). While those two variables helped to conceptualize the Artifact Truth Bias construct, they will not be considered for this current research project as they do not directly apply to the research questions. This will be examined in future research endeavors. Thus, Artifact Truth Bias will be presented as the first independent variable.

Artifact Truth Bias is an independent variable with a negative influence on Deception Detection Ability. Similar to human-to-human truth bias noted in Chapter 2, it is the result of heuristics that artifact users use to evaluate the reliability of the information source. In this case, that source is the artifact in use. For the purpose of this study, Artifact Truth Bias is defined as the level of trust and perceived reliability a given user has toward a specific artifact. While it is certainly possible that users can form the perception that a given artifact is not reliable and is untrustworthy, this study assumes that artifact users most often come to rely on artifacts and develop some level of truth bias. As noted in the literature, truth bias, in human-to-human relationships, results in an increased vulnerability to deception.

In summary, the truth bias construct is derived from a user's experiences with artifacts in general and from their experience with the artifact in use. Likely this

experience is mostly non-negative and users establish a truth bias or perception of reliability regarding the information derived through the artifact channel. Because of that truth bias, users become complacent and accepting of the information they receive from the artifact, their vulnerability to deception goes up, and their ability to detect deception is reduced. Thus, in artifact-human relationships:

**H1: Artifact truth bias is negatively related to deception detection ability.**

Since this research is concerned with increasing user deception detection ability, some variables positively influencing the dependent variable have been included in the research model. There are three variables, all well supported by the literature that may have a positive effect on user Deception Detection Ability. The first variable is User Experience in the Domain. This variable is defined as a given artifact user's knowledge of the information and data in the realm in which they are working. Highly experienced users should be very familiar with the information and data used in their task domain and how it is related to other information and data. User Experience in the Domain incorporates the user's knowledge of what information and data should be available, how the data or information is typically supposed to look and interrelate, and the typical location of certain data items in the artifact domain. In short, experienced users in the domain have a clear understanding how things should look in a normal situation (e.g. a situation free of errors or deceptions).

Thus, users with more experience in the domain should be better at detecting deceptions than users who are new to the domain. This should also be true even if the

novice is well-versed with artifacts in general. The fact that the experienced users know how the information should look should provide them with greater ability to detect deception, simply because they would better know when something in the information is out of the ordinary. With such an understanding of the domain:

**H2: User experience in the information domain is positively related to user's Deception Detection Ability.**

A second variable that should help all artifact users, experienced and novice alike, to increase their deception detection abilities, is arousal. If artifact users are aroused to the fact that the information derived from the artifact may have been compromised, their level of vigilance should increase and, in turn, their level of detection ability should increase (Parasuraman, 1984; Klein, et al., 1997). If the vigilance decrement situation is indeed true (Mackworth, 1950; Wiener, 1987), then arousal of users to the possibility of deception should increase their ability to detect deceptive signals in the regular data noise.

**H3: Arousal (producing expectations of possible information manipulation) is positively related to Deception Detection Ability.**

A final variable that should influence users' ability to detect deception in information derived from the artifact is Detection Training. Johnson, et al., (1993) demonstrated, on a limited basis, that auditors could improve their fraud detection capability if they were trained on Bowyer's taxonomy of deception tactics as they relate to the accounting field (Bowyer, 1982). The taxonomy (described in Chapter 2) is rather

generic and can be applied to any field or artifact domain. Thus, if a training program was developed in an artifact domain to help users identify the signals of deception in the information provided by that artifact, it could have a profound effect on deception detection capabilities.

#### **H4: Deception Detection Training is positively related to Deception Detection Abilities.**

By training artifact users to understand the taxonomy of deceptive practices, users should better be able to accurately detect strategic information manipulations. However, one question remains: Which factor or method for improving Deception Detection Ability is best? User Experience in the Domain is important to Deception Detection Ability as users need to understand or have a feel for how the data or information produced by the artifact would look under non-deceptive conditions (Davies and Tune, 1969; Campbell, 1990). Signal Detection Theory would suggest that experienced users have a better sense of what is signal and what is background noise. On the other hand, Aroused Suspicion to the possibility of deception should increase vigilance. However, since the goal of this research is to improve correct detection of deception, arousal may not be as influential since it has been shown to increase the number of false alarms (Parasuraman, 1984). Detection training would likely prove to be effective, as not only would the users be aroused by the fact that they are receiving such training, but it also would teach them the signals of deceptive practices (Johnson, et al., 1993). While the training and arousal may not bring the novices to the detection level of experienced users,

it should increase their ability to notice some signal patterns out of the background noise.

The following additional hypothesis is offered to address these issues.

**H5: User Experience in the Domain combined with Deception Detection Training and Arousal will provide greater positive influence on Deception Detection Ability than will Arousal, Deception Detection Training or a combination of the two.**

Currently, there is insufficient theoretical or empirical evidence to support hypotheses regarding interaction effects between User Experience in the Domain, Detection Training, and Arousal. However, this research will endeavor to explore such interaction effects as it may provide useful information toward future theory building work in this area of study.

Past research on deception and deception detection has focused on arousal. Except for Johnson, et al., (1993), very little has been accomplished toward developing a method of training for deception detection. While Johnson and his colleagues examined the field of accounting using paper based audit methods and certified auditors as subjects, this research differs in a number of ways. First, the objective is to better understand the relationship between information artifacts and the people that use them. The subjects of the study will receive the information they need to make decisions directly from the artifact. Second, Johnson used professionals (auditors) whose job is to find discrepancies in the information presented to them. This study will focus on subjects in the course of their daily duties who do not have an explicit mandate to locate deceptions in the information they use. Third, Johnson, et al., (1993) used three similar



subjects for their research in a case study methodology. This research endeavor will examine significantly more subjects.

In short, the goal of this research is to determine the influence of truth bias on artifact-human associations and examine methods for counteracting the potential vulnerabilities of such relationships. In order to do this, the research must examine the characteristics of the artifact users, their attitudes toward both computers in general and the specific system(s) they use to complete their daily tasks, their detection abilities without arousal, and their abilities when aroused and when trained. Information Manipulation Theory (McCornack, 1992) and truth bias (McCornack and Parks, 1986) play a key in understanding deception vulnerabilities. Signal Detection Theory (Davies and Tune, 1969) provides the theoretical foundation for examining the detection methods. A research model and hypotheses were developed in order to examine the phenomena. The next step is to incorporate an appropriate methodology for examining the hypotheses. The following chapter illustrates the methodology for capturing the necessary data needed to test the presented hypotheses.

## **CHAPTER 4**

### **METHODOLOGY**

Considering the nature of the hypotheses offered above, an empirical investigation was designed such that an artifact-user relationship could be examined. Further, the relationship was one where the user had a perception of reliable use toward the artifact. That is, the conditions had to be right for a truth bias to develop. Thus, the research site had to demonstrate that the user had a familiarity with the artifact, much like receivers have familiarity with senders in interpersonal relationships (Burgoon, et al., 1996; McCornack, 1992).

#### **Proposed Site**

A laboratory experiment with an augmenting survey instrument was used for the investigation. This required a site where respondents could interact with an artifact that was familiar to them. The advantages of the augmenting survey include the ability to query multiple respondents and lower cost. The disadvantage, as is often reported, is the possibility of a poor response rate. The advantages of a laboratory experiment include the ability to control the experiment, ease of data collection, and ability to use a control

group. The disadvantage is that an adequate setting for the study may be hard to find. This study combines the two research methods at a real world training site allowing for the best of both methods while adding realism. The proposed site is described below.

Keesler Air Force Base (KAFB) is one of a few Air Force installations designated as a training base. The 335th Training Squadron is a unit at KAFB with a mission to train Air Force members in the Personnel career field and other career fields. Enlisted personnel specialists often receive two units of training at KAFB. The first is conducted shortly after they enter the Air Force, immediately following basic training. The second opportunity to receive training arises after these individuals have been in the service for five to seven years. This second unit of training is designed to give the Personnel specialists up-to-date information regarding new tools and techniques used in the career field. Officer Personnel specialists receive only their basic career field training at the 335th.

### **The Information System**

A key information system used by personnel specialists throughout the Air Force is an information system called Personnel Concept III, better known in the field as 'PC-III.' Enlisted personnel specialists are trained on PC-III during their initial training, and they work with it throughout their careers. They receive even more instruction when they return for their next level of formal training typically at the five to seven year point. Officer personnel specialists receive only initial PC-III training at the 335th. PC-III is an information system and database that contains much of the unclassified personnel

information on nearly all Air Force members and civilian employees. This information can include name, rank, duty title, career field skill level, education level, other career fields for which a member might be qualified, assignment preferences, and a host of other information. PC-III is also interfaced with financial databases that control military and travel pay for active duty Air Force members.

PC-III is an information system that has been in use by the Air Force for several years. The personnel specialists who use PC-III have developed a familiarity with the system and have come to rely on it for nearly all of their personnel information processing needs. Alternative approaches for meeting their information processing needs are difficult to access and must often be relearned. Thus, PC-III was an excellent instrument for the study at hand.

Another advantage of using the PC-III system is that a laboratory already exists to conduct the experiment. The 335th Training Squadron houses a complete mock-up of the PC-III system. It is a stand-alone network that instructors can manipulate by running various programs. It provides for the same interface as the real PC-III, and it may be safe to say that many of the new and returning students are unaware that it is not connected to the real system. Thus, the PC-III training facility provided for an ideal environment to test the hypotheses listed above.

A final advantage to the PC-III laboratory is that strategic manipulation of information in the system can be accomplished quite easily. PC-III system administrators can access the laboratory system and make changes to the various records it contains.

For example, a lab administrator can enter the system and give a particular Air Force member (in the system) a new assignment, extra awards and decorations, or record of derogatory administrative actions (e.g. admonishments, reprimands, non-judicial punishment). Such manipulations can simulate a hacker entering the system and making changes to disrupt the orderly flow of operations.

### **Study Design**

The study took place in two parts. A field experiment was used to capture the necessary data for Hypotheses 2 through 5. An augmenting survey instrument was used to obtain an independent measure of Artifact Truth Bias and evaluate Hypothesis 1. The survey also provided the means to collect data regarding the experience level of the subjects. Additional surveys were administered as well. The surveys were completed first, then the respondents were subject to the experiment the next day. So as not to arouse the respondents to the true nature of the study, they were told that the survey and following experiment were for the purpose of adding more real world, scenario-based training to the course curriculum. Specific details regarding the experiment and augmenting survey of this study are provided in the sections below.

### **The Experiment**

As noted above, the primary mode of study was a laboratory experiment using PC-III. At the 335th, there are two types of personnel courses: Personnel Specialist

courses and Personnel Systems Management courses. The Personnel Specialists are the *users* of PC-III and the information it contains. Their duties include inputting information into the PC-III database and using the information to make decisions about the lives of airmen throughout the Air Force. These decisions can range from determining duty assignments to selecting personnel to attend in-residence professional military training (often considered a prestigious and career enhancing opportunity), to reporting personnel as eligible or ineligible for promotion or re-enlistment. In short, PC-III and the people who use it have a significant impact on the lives of thousands of Air Force members. Strategic information manipulations as described by Zmud (1990) could have, if undetected, serious implications for many people.

Personnel Systems Management specialists (PSMs) are the *maintainers* of PC-III. They are responsible for the maintenance and administration of PC-III. At the training facility at the 335th (often called the "schoolhouse"), the PSM instructors have supervisory authority of the PC-III training mock-up. That is, they have the ability to manipulate any and all of the information in the system. For the experiment, the PSM instructors manipulated the data used by the users.

There are essentially three groups or types of individuals or users involved in this study: Officer, Apprentice, and Craftsman. Those in the Officer groups are typically college graduates (Bachelor's degree required); have attended the Air Force Academy, the Reserve Officer Training Corps (ROTC), or Officer Training School (OTS); and have been appointed a commission in the United States Air Force. Officers typically have had

some formal computer training while in college. Occasionally, some officers have prior enlisted experience or are cross-trained from other career fields.

Those in the Apprentice group are high school graduates who recently enlisted in the Air Force. While some in this group may hold college degrees, the typical Apprentice has no formal education beyond high school and little formal computer training. However, some students in the apprentice course may be retrainees from other career fields. Those in the Craftsmen group are typically noncommissioned officers (NCOs) in the Air Force who are experienced in the personnel and PC-III domains. Many hold college degrees and all must have completed on-the-job-training (OJT) throughout their careers in order to qualify for the Craftsman course. Most have had either formal training or OJT on PC-III and are experienced computer operators as the Air Force as become extremely automated in the past decade.

It was necessary to use all three groups for a number of reasons. First, the three groups represent the population of Personnel specialists in the Air Force. Removing any one of them would detract from the representativeness of the study. Second, one of the groups has significant experience in the domain while the other two do not. Using multiple groups supports some of the hypothesis testing. Third, examining groups with various computer familiarities may prove useful in the author's future research endeavors. Finally, the 335th Training Squadron leadership expressed an interest in study and course supervisors requested that their courses be included.

All three groups of users receive some form of PC-III training at the 335th, and all access the same PC-III database to accomplish their course-related tasks. For the experiment, the systems administrators strategically manipulated the information accessed by the users in each of the three groups, and the users' abilities to detect the staged deceptions were recorded and measured. Considering that three types of users are involved and each was examined in normal, aroused, and trained capacities, a matrix design may best suit the needs of the study. A matrix design seemed to help in the organization of the experiment and appears to be conducive to the statistical manipulation suggested below. The next section outlines such a matrix design.

### **The Matrix Design**

Based on the research model offered in Chapter 3, a four-group, pretest-posttest design was used (Cook and Campbell, 1979). The four groups were obtained from the different classes of each subject type 'on board' at the time of the study. Usually, all of the personnel courses have two or three classes running simultaneously. There are no special classes offered and students are picked based on their availability to meet class dates. There is little variation from one class to the next. In short, the classes are rather homogeneous.

One class for each of the three group types (e.g. officer, enlisted, craftsman) was subjected to the experiment as either a controlled group, an aroused group, a trained



group or an aroused-trained interaction group. The model of the laboratory experiment is depicted in Figure 4-1 below.

	Control	Aroused	Trained	Interaction
Officer				
Apprentice				
Craftsman				

**Figure 4-1 - Laboratory Experiment Model**

In a typical Personnel classroom, students are required to accomplish a battery of exercises using PC-III or a PC-III simulator. The scenarios for each of the groups are tailored toward the tasks the students will perform at their next duty station. Sometimes, instructors share task ideas with instructors in other groups so as not to reinvent the wheel. Also, all of the students, no matter what group they are in, access the same database. A synopsis of the classroom scenario and data manipulation is presented in the next sections.

## **Classroom Scenario**

In a typical classroom setting, students are assigned to a workstation, given a handout containing the PC-III tasks they must perform, and are given an established time limit in which to complete their assignments. The average classroom size is 16 students. While the students are not evaluated on the speed with which they perform the tasks, only a finite period of time is allowed, as PC-III instruction is a subset of each of the three types of courses. Students are generally required to work alone, but if a student has a problem, a good idea, or an extra learning experience avails itself to the class, discussion is allowed. Students are also informed at the beginning of their courses to identify and report to instructors any discrepancies they find in the course material. This corrective action can be taken swiftly. However, it would not be seen as unusual to instruct students that portions of the course require independent work on the part of the students, and classroom discussion is prohibited.

## **Data Manipulation**

For the purposes of the experiment, students were given a set of scenarios reflecting typical decision making tasks that the students accomplish on the job. However, the PC-III data was strategically manipulated to influence the students to make flawed decisions regarding the decision-making tasks they must accomplish for the course. Each of the assigned scenarios is provided in Appendix A. A description of the task performed and an explanation of the data manipulated is provided in Appendix B. Also, views of the various PC-III screens used by the students are presented in Appendix

C. Students were instructed to work on their own without classroom discussion for the duration of the task. In all groups, students were provided with a discrepancy sheet with which to report any discrepancy noted in the data. The discrepancy sheet was the main source of recording the students' ability to detect the information manipulations. The use of the discrepancy sheet was not considered unusual to the students as it is used throughout their courses. However, there was one difference. The discrepancy sheet for the study contains a time stamp (5 minute intervals) and students were asked to note the point where they found a problem. They were told the time stamp was added to aid instructors' efforts to find and fix the problem at a later date. A copy of the discrepancy recording sheet is provided in Appendix D.

For each to the courses, a series of data manipulations was incorporated into the database by the PSMs who administer the system. One of the main concerns involved determining how much information to manipulate. Too many manipulations and the students may catch them on chance. Too few manipulations might result in few or no findings. Past work on data error detection manipulated approximately one third of the records reviewed by subjects (Klein, et al., 1997). However, strategic information manipulation is different from data errors in that the manipulator has a goal of influencing the information user's decision making outcomes. Furthermore, in PC-III, system edits prevent many data errors from occurring. Therefore, each manipulation must be crafted such that it influences decision makers, yet still remain within the confines of those edits. Also, the students only had a finite amount of time to complete

their tasks (approximately 90 min). The students were tasked to act on a series of 20 scenarios in which they were required to look at the records of one to four airmen and make decisions that might influence the airmen's careers. Of the 20 scenarios, 15 contained records with manipulated information that may cause the users to make incorrect decisions regarding the airmen. The other 5 scenarios contained records with no manipulations. If the students happened to notice too many scenarios with problem records, it could have jeopardized the study. Thus, three-fourths of the scenarios involved deceptions, but only 22 percent of the records will include strategic manipulations. A strategy of manipulation difficulty is provided in Appendix E.

Originally, the experiment was designed for a 2 hour time period with 17 of 25 scenarios containing manipulated data. However, a pilot study was conducted, and it was discovered that changes needed to be made. First, the courses are required by 81st Training Group regulations to allow for breaks every 90 minutes. The students have become accustomed to these breaks and become irritated when they are not on the schedule. Second, the course instructors requested shortening of the experiment time. While there is room built into each course for guest speakers and special events, that time is not infinite. Third, the pilot group of students reported that although they were accustomed to working under pressure, they felt 25 scenarios were just too many. Thus the decision was made to shorten both the experiment length and task number to the extent reported above. Finally, most of the students who were novice users of PC-III wasted a lot of time hunting through the various screens to locate a particular piece of

needed information. To prevent this problem, the names of the screens where needed data is located were noted at the end of each scenario.

Another concern involves the obviousness of the manipulations. Manipulations that are too obvious may be easily found by all test groups. However, if the manipulations are too discrete, very few would find them. The manipulations cover a scale from easy to difficult to detect. During scenario building and record manipulation, instructors of the different student groups provided insight as to what manipulations they felt their students might detect. As expected, instructors of the novice students (airman and officers) indicated that their students would find many of the manipulations hard to detect. This, however, is assumed to be a good sign as it may better test the validity of the detection training. See Appendix E for a further discussion of the data manipulation strategy.

These manipulations were based on the taxonomy used by Johnson, et al. (1993). While one of the tacit goals of this research is to learn if the taxonomy could be used to build a deception detection training program for artifact-produced information, it should be understood that not every artifact may be manipulated in all of the ways described in the taxonomy. Certain redundancy checks (known as "edits" by the PSMs) and data entry standards in PC-III prevented the use of some of the manipulation methods. However, every attempt was made to follow the taxonomy and manipulate the data as much as possible to represent each of the seven methods. The students were then put through the treatments as described in the section below.

## **Control and Treatment Groups**

The Control groups were put through the paces of the PC-III tasks without any input. They were not aroused nor made aware in any way that there was something different about their PC-III training. They were assigned their tasks, given their discrepancy reporting sheets, and informed that this portion of their training was to be accomplished independently without any discussion with classmates. If students felt they must bring a problem to the attention of the instructor (researcher), they were allowed to do so, but that is all. The students were instructed to turn in all their materials upon completion or at the end of the time period. In short, this group did not experience anything different than their normal routine. The treatment groups will be subject to changes from the norm.

The first treatment group in each of the classes was the aroused group. This group was informed at the beginning of the experiment that someone (e.g., a hacker, a disgruntled PSM student) had been tampering with the course data. They were told that they were still required to work alone, but they should definitely record any problems on the discrepancy recording sheet. Other than the heightened state of arousal, they proceeded through their assigned tasks much like the control groups.

The second treatment group was the trained group (also referred to as the trained-only group). The students underwent a short training program taught by the researcher that instructed them on the deception methods highlighted in the taxonomy. To ensure the students would not be aroused by the presence of the researcher and the training,

precautionary measures were taken. The goal of this treatment was to learn if training alone can improve the deception detection capability of the students. Care was taken to ensure the students were not aroused by the training itself. First, the researcher wore his uniform and master instructor badge at all times in the training facility. Second, the students were informed that the researcher was there to provide them with some additional computer security awareness training due to some recent hacker attacks on Air Force information systems. Conveniently, the news media had recently run an Associated Press article reporting a hacker break in to Air Force personnel and financial systems at the Pentagon! This made for an opportune introduction into the taxonomy training. Third, the researcher developed a training lesson plan in accordance with the Air Force's Air Education and Training Command guideline. If a student happened to see the training materials, he or she would simply see another course lesson plan. A copy of this lesson plan is in Appendix F.

In all three types of classes (e.g. officer, apprentice, and craftsman), students are required to have an instructional unit on Communications Security (COMSEC). This instruction is typically held early in the courses while computer instruction (e.g. PC-III) is near the end. For this treatment, students received their training on the taxonomy during COMSEC instruction, but heard no more of it for the remainder of the course. Because the two parts of the courses are distant in time of occurrence, students were not roused to the manipulations in PC-III. As with the other groups, respondents recorded any possible problems on the discrepancy recording sheet.

The final treatment group received the training mentioned above and was aroused right before the experiment was to take place. Instead of receiving their training during their COMSEC instruction, students in this group were trained at the time of their PC-III instruction, and they were aroused to the fact that some of the information they were seeing had been manipulated. In this way, the interaction of the training and the arousal could be considered.

Once the experiment was complete, the researcher had a set of discrepancy recording sheets from each group so as to complete the matrix depicted in Figure 4-1. For an alpha of .05, the appropriate sample size for the population of Personnel specialists should be 200. However, since there were typically 16 students per class and 12 classes were involved in the study, this approach would only yield approximately 192 subjects. That is approximately 8 students short of the calculated sample size. Doubling the classes in each box of the matrix was not an issue. While the researcher was given liberty to use the classes, the generosity of the squadron was not without end. It turned out that the Craftsman courses had more classes on board in this period. Since one of the goals of the study was to determine whether experience in the information domain makes a difference, and that there were significantly fewer subjects in the experienced groups than the non-experienced groups, the extra courses were used.

A two-factor randomized block design analysis of variance was used to examine the data. Tukey's Honestly Significant Difference (HSD) test was also used for evaluating specific group differences. However, this experiment only encompasses part



of the research model. The results of the experiment were designed to exhibit differences in each of the groups so as to provide evidence in favor of one of the detection methods. For example, it could be that arousal alone is sufficient enough to increase deception detection. Or, it is possible that the craftsman students with their greater experience in the PC-III domain will be more successful than the aroused and or trained groups with less experience (e.g., officer or apprentice). Therefore, the experiment will help to determine the group that performs best and, in turn, aid in future endeavors to help users of PC-III detect deceptions. Still, it does little to aid the understanding of the role of truth bias in deceptive information practices via artifacts. In order to measure that portion of the research model and its corresponding hypotheses, a set of scales was used to augment the laboratory experiment. The use of the scales is described in the section below.

### **The Attitude Scales**

Much of what the users of PC-III believe about its reliability and trustworthiness is derived from their past experiences with both PC-III and other artifacts in general (Tversky and Kahneman, 1974). Figure 3-1 illustrates how truth bias may develop from these experiences. In order to examine Hypothesis 1, it is necessary to learn if the users' have a truth bias toward PC-III. For the purpose of this research it is assumed that users reporting a higher perceived reliability of PC-III will have higher levels of truth bias toward PC-III and lower levels of deception detection performance.

To capture the users' perceived reliability a PC-III trust scale has been developed (Appendix G). A review of the literature found very little to offer in terms of existing scales to measure the level of trust by a human toward an artifact. Past research has demonstrated how person-to-person relationship research can be adapted to artifact-human relationships. In fact, such adaptations can be found in research on human intervention in automated systems (Muir, 1994), the design of decision support systems (Muir, 1987) and on human-computer cooperation (Moray, et al., 1995). However, little, if any work has been accomplished on scale development to examine human trust of artifacts. The trust scale in Appendix G is an adaptation of Rempel and Holmes Trust Scale for measuring trust in close relationship (Rempel and Holmes, 1986).

There are other trust scales involving a specific other, such as the Johnson-George and Swap Measurement of Specific Interpersonal Trust (Johnson-George and Swap, 1982). However, the Rempel and Holmes scale appeared to offer more adaptability to the study at hand, and it is reported to have sound empirical support of its validity and reliability (Rempel and Holmes, 1986). The original scale is comprised of three sub-scales involving: predictability, dependability, and faith. Each item on the scale uses the term "My partner" when referring to a specific other in a close relationship. For the purpose of this study, the term "My partner" was replaced with the term "PC-III" for each scale item. Further, after review of the scale items, it was determined that the items in the faith sub-scale were irrelevant to the current study. However, it is important to note

that the level of validity and reliability were report by Rempel and Holmes as nearly equal for all sub-scales and the overall scale (Ibid.).

In order to evaluate the influence of truth bias on deception detection, the study uses the survey results to obtain the perceived truth bias level for each of the respondents and the experiment results to determine their deception detection abilities. It is hypothesized that those individuals deemed to have higher levels of truth bias will demonstrate a lower level of deception detection performance. Users who perform lower in the experiments and have a high reported perception of reliability toward the information they receive from PC-III are assumed to be influenced by truth bias.

In addition to the PC-III trust scale, a short questionnaire was used to measure the students' experience in the information domain (i.e., Hypothesis 2). The questionnaire is comprised of a number of questions to elicit information from the students regarding their depth and breadth of experience in the Personnel career field. This measurement instrument was created with the aid of Personnel instructors who provided input as to what they would want to know about the students' experience level. The resulting measurement should provide an independent measure of Experience in the Domain from which to evaluate Hypothesis 2.

In the end, the experiment and surveys attempt to help explain who is likely to have higher levels of truth bias, the influence of truth bias on deception detection, and how different methods of increasing deception detection will affect the outcome. A

discussion of results and analysis of the experiment and survey instrument is presented in Chapter 5.

## **CHAPTER 5**

### **RESULTS AND ANALYSIS**

This chapter describes the results of the experiment and corresponding survey introduced in the preceding chapter. All told, 205 respondents participated in the experiment and provided information via the survey. Since the survey provided the necessary information to answer Hypothesis 1 of the research model depicted in Chapter 3, analysis of the survey results will be conducted first. Then, the results of the experiment will be analyzed to determine the outcomes of the remaining 4 hypotheses.

#### **Survey Findings**

The purpose of the survey was to provide for an independent measure of truth bias toward an artifact (e.g. PC-III). The survey was administered to three distinct groups of Air Force Personnel Specialists. Sample statistics including number of respondents per group, average depth and breadth of experience in the field, and a group mean of attitude toward PC-III derived from the modified Rempel-Holmes scale are provided in Table 5-1 below.

**Table 5-1 - Summary Statistics of Survey Findings**

	Control	Aroused	Trained	Interaction
Officer	n = 16 d = .88 b = .81 u = 3.04	n = 15 d = 1.47 b = 1.53 u = 2.83	n = 16 d = 1.56 b = 1.06 u = 3.09	n = 15 d = .86 b = 1.00 u = 2.92
Apprentice	n = 17 d = .41 b = .41 u = 3.27	n = 17 d = .41 b = .24 u = 3.18	n = 15 d = .20 b = .20 u = 3.15	n = 16 d = .38 b = .25 u = 3.31
Craftsman	n = 21 d = 6.29 b = 3.10 u = 3.52	n = 19 d = 6.84 b = 2.84 u = 3.41	n = 19 d = 6.11 b = 2.68 u = 3.18	n = 21 d = 6.10 b = 2.48 u = 3.11
n = number of respondents in group      b = number of areas worked in Personnel field d = number of years in Personnel field      u = group mean attitude of trust toward PC-III				

**Group Size**

As noted in Chapter 4, typically the typical class size for all Personnel courses is 16. Course supervisors usually receive their class rosters about a week before each class is to commence. The roster is nothing more than a short listing of student names, ranks, and social security numbers. Other than that, nothing more is known about the incoming classes. While the typical class size is supposed to be 16, unit deployments, personal problems, administrative oversights, and other general scheduling mishaps often vary the number of students attending a given class. In the case of the officers' courses, the aroused group and the interaction group each contained a member who did not meet the sampling criteria. The aroused group had a civilian student in the class and the

interaction group had a foreign national in the class. During the course of the experiment, these students were allowed to work on other course material in the student lounge.

The apprentice courses had similar changes in their size. Two of the courses had 17 students (as scheduled on the roster), while one course had 15. One student who was supposed to be in the aroused group was "washed out" of his Basic Military Training (BMT) course for failing to meet Air Force standards.

The Craftsman courses had the largest amount of changes from the scheduled rosters. In retrospect, this is not unusual as the noncommissioned officers (NCOs) attending these courses are older, have more responsibilities at their home units, and they have more family issues to consider. During the course of this study, the average craftsman course class size was either 13 or 14 students. However, it turned out that the Craftsman course had two courses running simultaneously on two occasions during data collection. In order to increase sample size, two extra classes were also administered the survey and subjected to the experiment. At the time of the experiment, each of the classes were informed that due to network difficulties, half would have to take the experiment in one classroom and the other half would use another classroom. This arrangement was easily accomplished for the controlled and aroused groups. As soon as the two sub-groups separated (the students chose the room they wanted to be in), the aroused group was provided the treatment (i.e., arousal to the fact that the data in PC-III had been manipulated).

Splitting a class to provide more subjects for the Trained and Interaction groups proved to be more challenging, but not impossible. As noted in Chapter 4, the Trained Craftsman group was to have its training a week prior to participating in the experiment (without arousal), and the Interaction Craftsman group was to be trained directly before the experiment (with arousal). Conveniently, at the time one of the extra classes was at a point to receive the training, the class had a guest speaker from the Air Force Personnel Center (AFPC). After his briefing, the guest speaker offered to spend 30 minutes conducting career counseling with volunteer class members. Seven class members took the offer. The other 6 members of the class were given the deception detection training based on the Johnson, et al., taxonomy (Johnson, et al., 1993). A week later the experiment was conducted. As the students entered the building for the experiment, the researcher greeted each one and explained that due to technical problems, they would have to occupy two rooms. When a student who had the training a week prior entered the building for the experiment, he or she was directed to one room. Students who did not receive the training were quietly directed to the other room, and they became part of the Interaction group. The rest of the experiment went as originally planned. The trained group subjects were told they were going to evaluate some real world exercises the courses were considering for inclusion into the curriculum and to note any discrepancies they saw. The Interaction group was given the training and aroused to the fact that PC-III had deceptive data. In a post-experiment discussion, the trained-only



students reported that they were completely unaware of anything suspicious going on. Thus, group integrity was not compromised and sample size was increased.

### **Experience Level**

Along with a measure of subject trust in PC-III, the experience level of the subjects in each of the three group-types was as captured as well. As part of the survey, subjects were asked how long they have been in the personnel career field and how many different areas in personnel have they worked for over 3 months. For the career depth measurement, a subject who reported being in the field less than 3 months would score a 0, 3 months to 1 year would score 1 point, one year to 2 years would score 2 points, and so on. For career breadth, subjects scored a point for each functional area in which they reported working in for over 3 months.

As expected, Apprentice students had very little depth or breadth of experience. The few that did report having experience in the Personnel field were interviewed after the experiment. Some were former Information Management (IM) troops that cross-trained into the Personnel career field. In command sections Personnel and IM troops share similar duties. In fact, according to Air Force news services, many more troops from the IM field will likely be merged into Personnel. Other Apprentice students reporting experience in the Personnel field were Social Actions troops. Social Actions is another field that is being consolidated with Personnel.

The Officer groups reported mean experience depths of 1 to 2 years and mean experience breadths of 1 to 2 areas. Thus, they have more experience than previously

expected. There are two reasons for these scores. First, due to a backlog of students, many of the officers did not get training quotas until after they had 3 months on the job. They worked in one of the functional areas for awhile at their bases and then were sent to the schoolhouse for formal training. Second, during post-experiment interviews, some of the officers reported that they were formerly in the IM career field and were cross-trained into the Personnel Career field. The Air Force formally merged the IM career field (at the officer level) into the Communications and Personnel Career fields approximately 18 months ago. Information Management Officers in positions that were merged into the Personnel field typically cross-trained into that field. The Air Force recognizes the officers' experience in those IM positions as equivalent to the same amount of experience in Personnel. Thus, they noted their IM time as Personnel time. This study also considered that time to be time spent in Personnel.

The Craftsman courses reported depth and breadth of experience as anticipated. They averaged about 6 to 7 years in the Personnel field with their time spent in an average of 2 to 3 functional areas. Some student reported having as many as 10 years in the field while other report as few as 2 or 3. This is not unusual. First, the Craftsman course is tied to rank. Some troops make rank faster than others. In post-experiment interviews, those who reported 8 or more years in the field also reported that it took them longer to make rank. As for those reporting 3 or fewer years in the field, they reported crossing-training into the field from specialties with similar functions and similar knowledge domains (e.g., IM, Services).

In summary, the selection of respondents by their course types appears to have adequately captured groups with sufficient differences in experience to make hypothesis testing possible. While the officer experience level was found to be higher than anticipated, this may prove beneficial to the study. Now, it is possible to consider three levels of experience: novice, some experience, and considerable experience. With sample size and experience considered, the next step is to look at trust toward PC-III.

### **Trust Toward PC-III**

The Rempel-Holmes Trust Scale discussed in Chapter 4 which is typically used to measure trust one human has toward a specific other was adapted to capture the level of trust users have toward a specific artifact. Essentially, the scale provides a space for a name of a significant other to be inserted into each of measurement statements. For the purposes of this study, the term "PC-III" was entered into the space provided. The scale then measures the respondent's attitude toward the reliability and predictability (i.e., trustworthiness) of PC-III. There are 14 items total in the scale and 7 items are worded such that the scores require reversals. All items are Likert-type and use a 5 point scale: 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree. Respondent answers to the scale were coded in an Excel spreadsheet and their means were calculated. As noted in Chapter 4, respondents' means of the scale items provide for an independent measurement of their perceived level of truth bias toward PC-III. As can be seen in

Table 5-1, group means indicate a tendency by subjects to remain neutral regarding their perceived trust in PC-III.

As expected, the Craftsman groups exhibited for the highest group means, indicating a slightly greater bias toward PC-III. This is especially true for the Craftsman Control Group and the Craftsman Aroused Groups. Information Manipulation Theory (McCornack, 1992) and the truth bias construct (McCornack and Parks, 1986) suggest that over time users should develop a greater truth bias toward PC-III. This may be true for some of the seasoned respondents in the Craftsman courses, however, calculating a Craftsman grand mean by combining all Craftsman respondent means yields a score of 3.35. An ANOVA was used to determine if the Craftsman groups had a truth bias measure significantly greater than the other groups. The results are depicted in Table 5-2 below.

**Table 5-2 - ANOVA of Reported Truth Bias Levels Between Group Types**

	Sum of Squares	ANOVA			
		df	Mean Square	F	Sig.
Between Groups	4.873	2	2.427	8.838	.000
Within Groups	55.689	202	.276		
Total	60.562	204			

A Tukey's Honestly Significance Difference test demonstrated that both the Craftsman groups ( $p = .000$ ) and the Apprentice groups ( $p = .019$ ) had significantly higher truth bias scores than the Officer groups. Thus, as Information Manipulation Theory suggests, the more experienced users did exhibit higher levels of truth bias than the less experienced users.

The existence of higher truth bias levels in the more experienced group is indeed relevant to this study. If the truth bias construct is correct for artifact/user relationships, then the Craftsman groups might be easier to deceive. However, while it is appropriate to see differences across group types, significant differences across treatment types would not be useful. They could confound the effects of the treatments. Fortunately, Table 5-3 illustrates that there were no significant differences in truth bias levels across treatment groups.

**Table 5-3 - ANOVA of Reported Truth Bias Levels Between Treatment Groups**

	ANOVA				
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.789	3	.263	.884	.450
Within Groups	59.774	201	.297		
Total	60.562	204			

Considering that there were significant differences among group types and not among treatment groups, the conditions seem to be appropriate to test the hypothesis. The group with the greater exposure to PC-III reported the highest level of truth bias toward the artifact. And, there were no significant differences between treatment groups. Thus, hypothesis testing appears to be in order. Since, the survey was used to gain the truth bias measurement for Hypothesis 1, further analysis of that instrument is in order.

### **Analysis of Survey Instrument**

Before any realistic analysis can be accomplished with regard to hypothesis testing, a review of the validity and reliability of the survey is necessary. The first portion of the survey (Appendix G) is merely a group of questions designed to collect information on respondents' level of experience in the Personnel career field. As noted earlier, this part of the survey was devised with the help of Personnel course instructors and seasoned members of the Personnel field (from here on, referred to as experts). These experts were asked how they would evaluate the career field experience and knowledge of the Personnel information domain of Personnel Specialists. They suggested time in the career field as a measure of depth, and provided a listing of functional areas as a measure of breadth in the field. The researcher, based on his Air Force experience, suggested a 3 month period should be considered as the minimum experience level for a functional area to be counted for the breadth measure. The experts

concurred with this amount of time, and it was used for score experience levels. Based on expert opinion, the researcher concluded that questions used to obtain the information as a measure of User Experience Level in the Domain (per Chapter 3, Fig 3-4) were appropriate and valid for this study.

The second part of the survey instrument is a series of 14 Likert-type statements used to capture respondents' attitude toward the truthfulness and reliability of PC-III. As noted above, these questions were derived from the Rempel-Holmes Trust Scale by placing the term "PC-III" in each of the statements where an individual's name is usually inserted. Since this scale has been designed and tested considerably in the past, it appears to be an appropriate measure for the study at hand. Course instructors reviewed the scale and found it to be appropriate for their students. As noted in Chapter 4, a pilot study of the scale produced encouraging results.

### **Scale Reliability**

The original Rempel-Holmes Trust Scale is reported to have good reliability with an  $\alpha = .87$ . A pilot study conducted before the experiment began reported higher reliability of  $\alpha = .94$ . The survey was administered to all groups on the day prior to the experiment. To ensure that groups were not aroused to the objective of the experiment the following day, they were told the survey was to get some preliminary data so that the course instructors might get a better understanding of students' attitudes regarding PC-III. As expected, many of the Apprentice students maintained that since they never really worked with PC-III outside the classroom, they found it difficult to answer something

other than neutral. Upon completion of the survey instrument, students were released for the evening. The experiment typically commenced on the afternoon of the next day. The researcher then brought the completed surveys back to his quarters and recorded the responses into data files. Reliability analyses were conducted on each the groups. Cronbach's alphas for all groups are depicted in Table 5-4 below.

**Table 5-4 - Alphas for Groups and Complete Sample**

	Control	Aroused	Trained	Interaction
Officer	a = .72	a = .85	a = .89	a = .72
Apprentice	a = .95	a = .84	a = .82	a = .85
Craftsman	a = .94	a = .80	a = .87	a = .88
Overall	a = .88			

The group alphas and the overall alphas appear to be moderately high to high. This indicates that the scale has high reliability in both groups and the total sample. Further analysis indicates that removal of any scale items would only produce marginal improvement in reliability. Also, a review of correlation matrices for the groups and total sample reliabilities revealed no extreme correlations.



Given the findings of the reliability analysis above, it appears, overall, that the survey instrument demonstrates moderately high reliability. This is not surprising given that it is a proven instrument. With these results in mind, it is time to continue the analysis and test the hypotheses introduced in Chapter 3.

### **Tests of Hypotheses**

Most of the hypotheses in this research endeavor were designed to be tested via analysis of variance (ANOVA). The experiment's design proved to lend itself quite readily to this method of data analysis. Furthermore, in situations where more than 3 groups were compared, Tukey's Honestly Significant Difference (HSD) Test was used to help confirm the findings and help determine which group means differed. The following sections will review each of the hypotheses and discuss the results of the findings.

#### **The Effect of Truth Bias on Deception Detection Ability**

The first hypothesis was created to examine the effects truth bias has on deception detection ability as asked by the first of the two research questions presented in Chapter 1. The hypothesis is restated as follows:

**H1: Artifact truth bias is negatively related to deception detection ability.**

To examine this hypothesis, an independent measure of user artifact truth bias was derived via the use of the survey instrument discussed above. A measure of deception

detection ability was taken by administering the experiment depicted in Chapter 4 to each of the respondents. Subjects reported all deceptive data on a discrepancy reporting sheet. The contents of the reporting sheet were then loaded into a data file for use in statistical analysis. All correct reportings of discrepancies were loaded into a field labeled "correct hits" and all reportings of items that were not discrepancies (i.e., false alarms) were loaded into a field label "incorrect hits." The two fields were then combined to form a third field labeled "total hits" and percentages of correct and incorrect hits were calculated. Occasionally, respondents reported as errors items that were legitimate errors in the PC-III database and not information manipulations that were 'planted' for the experiment. Discussions with Personnel Systems Administrators (PSMs) confirmed these errors and they were filtered out of respondents' scores at the time the data was coded into the data files. Once the experiment was completed for all groups and the data was loaded into files, the analysis of Hypothesis 1 commenced.

The first part of the analysis came in the form of a regression. Simply put, respondents' scores of correct hits was the independent variable and respondents' mean scores on the survey and a dummy variable of 12 classifications to divide the groups were the independent variables. The objective was to learn how much of the variability in correct scores could be explained by the truth bias measure (mean score on the PC-III trust scale). The regression analysis yielded an  $R^2 = 10.4$  suggesting that the truth bias measure is not a very good predictor of a respondent's ability to correctly identify deceptive data in PC-III.

The second part of the analysis compared the means of correct scores between respondents reporting low, neutral, and high levels of truth bias. This had to be accomplished in such a way that the treatments could not confound the analysis. The data was divided along treatment lines. All control, aroused, trained, and interaction respondent scores for correct hits and mean survey scores were placed in separate data files and all survey scores (truth bias scores) were coded with a 1, 2, or 3 to reflect low, neutral and high truth bias respectively. Mean scores for correct hits for each treatment group at each truth bias level are depicted in Table 5-5 below.

**Table 5-5 - Mean Correct Hit Scores By Truth Bias Level**

	Control	Aroused	Trained	Interaction
Low TB	1.40	2.64	0.53	3.77
Neutral TB	0.81	1.30	0.22	2.33
High TB	0.68	2.59	0.77	3.16

It appears that in all, but the trained treatment groups, those respondents with lower levels of truth bias as measured by the PC-III Trust Scale performed only slightly better than those reporting higher levels of truth bias. In the Aroused and Interaction treatment groups, it appears those respondents reporting high levels of truth bias performed better than those reporting neutral levels. However, it is important to note that the majority of the neutral scores came from the Apprentice Personnel respondents who generally do not perform as well as the more experienced Craftsmen Personnel respondents. This matter of experience will be discussed later in the chapter.

Since differences in mean scores did exist, ANOVAs were conducted to determine if the differences were significant. A review of Table 5-5 above would probably suggest to a trained eye that the differences in means were not significant. However, the ANOVAs were conducted just to make sure. In all cases, F-tests indicated that no groups reporting lower levels of truth bias did significantly better (or worse) than groups reporting higher levels. Only the ANOVA for the Aroused groups indicated a difference at the  $p=.06$  level, but that was not enough to lend support to the hypothesis. Since no significant differences in means were found, further analysis such as Tukey's HSD was not considered.

Such findings might call into question the validity of the scale as a measurement of truth bias. However, all respondents also were administered two other scales in an attempt to gain a better understanding of their attitudes toward computers and PC-III data quality. The first scale administered was the Attitudes Toward Computer Usage Scale (ATCUS) (Popovich, et al., 1987). This is a 20-point scale that has been independently validated and administered to a variety of groups (Brown, et al., 1988; Koslowsky, et al., 1988). The second scale is a 7-item semantic differential measuring the single factor of user perception of PC-III data quality. Both of these scales are presented in Appendix H.

The data collected from these two scales was loaded into data files. The results of the three scales combined should capture respondents truth bias toward PC-III as they measure attitude toward computers in general and provide two measurements of attitude toward (or trust in) PC-III. However, together they provided for only a minimal increase

of success as a predictor of deception detection ability. Reliability analyses were conducted on each and a Pearson Correlation test was administered for all three scales. This data is represented in Table 5-6 and Table 5-7 below.

**Table 5-6 - Reliability Analysis of the Scales**

	PC-III Trust Scale	PC-III Data Quality Scale	ATCUS
Reliability (Alpha)	0.88	0.94	0.71

**Table 5-7 - Pearson Correlation of the Scales**

Scale	PC-III Trust Scale	PC-III DQS	ATCUS
PC-III Trust Scale	1.000	0.482**	0.162 *
PC-III DQS	0.482**	1.000	0.211**
ATCUS	0.162 *	0.211**	1.000
* Correlation is significant at the 0.05 level.			
** Correlation is significant at the 0.01 level.			

Descriptive statistics from the additional scales were calculated and compared to the PC-III Trust Scale. The mean, median, and mode for each of the scales is provided in Table 5-8 below. In both the PC-III Trust Scale and the PC-III Data Quality Scale, the mode statistic indicates that many of the respondents were neutral with regard to PC-III trustworthiness. However, most of the respondents reported high scores for the ATCUS as multiple modes calculated above 4.1 on a 5-point scale. The respondents reported positive attitudes to computers in general, but were more conservative with respect to PC-III. In similar manner to the PC-III Trust Scale, ANOVAs were completed

in the additional scales. These, too, failed to find significant differences in performance between those who reported low, neutral, and high scores on the additional scales.

**Table 5-8 – Descriptive Statistics of All Scales**

Scale	Mean	Median	Mode	N
PC-III Trust Scale	3.2003	3.0714	3.00	205
PC-III DQS*	5.2983	5.4286	4.00	205
ATCUS	4.1985	4.2000	4.10-4.50	205
* Indicates a 7-point scale				

In sum, regression analysis suggests that the PC-III Trust Scale as a measure of truth bias is not an adequate predictor of truth bias. While a review of the data indicates some differences in group means, ANOVA indicated that the differences are not significant. Based on that evidence, Hypothesis 1 cannot be supported. Given that the truth bias scale seems to measure its underlying construct (as evidenced by Table 5-5), this result does not seem attributable to measurement problems. Suggestions as to why there is a lack of support for Hypothesis 1 will be discussed later in the chapter. The analysis of the data used for testing Hypothesis 2 will be considered next.

### **The Effect of Experience on Deception Detection Ability**

The remainder of the hypotheses were created to answer the second research question presented in Chapter 1. Specifically, it asks what factors can improve deception detection performance. Hypothesis 2 is the first to examine a specific factor for improving deception detection in artifact users: User Experience Level in the Domain. For convenience, Hypothesis 2 is reiterated below:

**H2: User experience in the information domain is positively related to user's Deception Detection Ability.**

As introduced in Chapter 3, it is hypothesized that the Craftsman specialist, due to their experience in the personnel information domain would perform significantly better at detecting strategic information manipulation than would the less experience Apprentice and Officer groups. As noted in Table 5-1, Craftsman group respondents typically have 6 or 7 years experience and have worked in 2 or 3 functional areas of the Personnel career field. Officers were found to have 1 or 2 years experience in 1 or 2 areas. The vast majority of Apprentice group respondents reported they had no experience in the field. However, a few retrainees reported experience in a Personnel functional area that used to be an Information Management Career field. This was accounted for in data collection and included in the Apprentice group's mean score.

An analysis of variance comparing the Craftsmen group performance (number of correct hits) to the less experience groups performance was accomplished next. The results of this ANOVA can be found in Table 5-9 below. As the noted in the table, there is a significant difference between the two groups at the  $p = .011$  level thus supporting the hypothesis that experience in the information domain is indeed related to a user's deception detection ability. When asked in post-experiment interviews why they felt that were successful at picking out deceptive data, there was considerable agreement on the reason. Many of the respondents explained that when they went into PC-III they had expectations about the data they were examining. When they saw a piece of data that

did not meet their expectations, they became suspicious of it. Apprentice students generally did not have preconceived expectations of what they were looking at. Many of the Officer respondents noted some expectations.

**Table 5-9- ANOVA of Experienced vs. Inexperienced User Deception Detection Performance**

ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	23.008	1	23.008	6.632	.011
Within Groups	704.289	203	3.469		
Total	727.298	204			
MEANS					
	Experienced		Inexperienced		
	2.17		1.48		

Since the Officer respondents did have some experience in the information domain, a second ANOVA was accomplished to determine if they might be significantly different from the Apprentice Group. Such a finding might help answer the question of how much experience a respondent may need to demonstrate better deception detection abilities. An ANOVA whereby the Craftsman group was compared to the Officer and Apprentice groups is presented in Table 5-10 below.



**Table 5-10 - ANOVA of Craftsman vs. Officer vs. Apprentice Groups**

ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	35.659	2	17.829	5.207	.006
Within Groups	691.639	202	3.424		
Total	727.298	204			
MEANS					
	Craftsman	Officer	Apprentice		
	2.16	1.80	1.17		

This analysis determine a difference in the groups' means with a significance of  $p = .006$ , however, it did not show which groups differ. A post hoc analysis using Tukey's HSD was performed. This test conducts pairwise multiple comparisons and will indicate which means differ significantly at a preset alpha level. For the purpose of this analysis, an  $\alpha = .05$  was used. The results demonstrated that the Craftsman group mean was significantly different than the Apprentice group mean at that level. However, no significant difference was found between the Craftsman and Officer groups or the Officer and Apprentice groups. A final ANOVA was accomplished comparing only the Craftsman and Apprentice groups. It resulted in a difference with a significance of  $p = .002$ .

In summary, the results of this portion of the experiment support the hypothesis that higher levels of experience in the information domain are positively related to a user's deception detection ability. How much experience is necessary remains to be seen. The Craftsman groups, with their considerable experience, performed significantly better than the Apprentice groups. However, differences in the Officer group with some experience in the information domain (1 to 2 years) and the Apprentice group were not found to be significant. Experience in the information domain does make a difference in deception detection performance of PC-III users. In the next section, the arousal treatment will be examined to determine its effect on such performance.

#### **The Effect of Arousal on Deception Detection Ability**

Klein, et al., (1997) noted that one of the reasons why people do not demonstrate a high error detection ability is due to the fact that they are unaware that it is required of them. The issue is also of concern to this research endeavor in the context of deception detection in artifact-produced information. The population of Personnel specialists is a highly trained group of professionals on whom the Air Force depends to provide timely and accurate attention to Personnel issues and records of all members. They do their job well and the Air Force personnel system can be argued to be the best in the United States military. However, while it is tacitly implied, Personnel specialists are not explicitly tasked to monitor for and detect strategic information manipulations in their information systems (e.g. PC-III). Therefore, the following hypothesis was offered to address this issue in the context of deception detection in artifact-produced information.

**H3: Arousal (producing expectations of possible information manipulation) is positively related to Deception Detection Ability.**

To test this hypothesis, many of the groups in the experiment were aroused to the idea that it is likely that there is deceptive data in the PC-III database. Like all of the other groups, the aroused groups were given their tasks to accomplish and told to record any discrepancies they found. Also, like the other groups, their data was collected and coded into databases. The data was then used in the following analysis.

Due to the experimental design, analysis of variance was the statistical approach of choice for this hypothesis. First, all groups that received the arousal treatment were compared to all groups without that treatment. Table 5-11, below, illustrates the results of the ANOVA.

**Table 5-11 - ANOVA of Aroused Groups vs. Non-aroused Groups**

ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	215.628	1	215.628	85.548	.000
Within Groups	511.669	203	2.521		
Total	727.298	204			
MEANS					
	Aroused		Non-aroused		
	2.78		.7308		

A review of the data tables shows the aroused groups have demonstrated a greater ability to detect deception than the non-aroused groups. The ANOVA resulting in the table above demonstrated that the differences in means of aroused versus non-aroused groups is significant at  $p = .000$ . This demonstrates strong support for Hypothesis 3. However, an ANOVA was also accomplished for the aroused-only groups and the control groups. Again, a review of the data reveals the aroused-only groups performed much better than the control groups. The ANOVA of aroused-only group versus control groups is presented in Table 5-12 below.

**Table 5-12 - ANOVA of Aroused-only Groups vs. Control Groups**

ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	57.316	1	57.316	28.418	.000
Within Groups	205.723	102	2.017		
Total	263.038	103			
MEANS					
	Aroused-only		Control		
	2.35		.8519		

As in the case of all aroused groups versus all non-aroused groups, the aroused-only groups did significantly better than the control groups at  $p = .000$ . This, too, lends support for Hypothesis 3. Arousal is positively related to deception detection ability.

While it has been demonstrated that arousal does lead to better deception detection ability in artifact-produced information, the issue of respondents' level of false detection remains. It was suggested in an earlier chapter that arousal may lead to more false alarms, thus reducing deception detection accuracy. During the experiment, respondent false detections were also recorded in the data files. As noted earlier, if a respondent noted a true error in the PC-III database, it was filtered out. Together, these steps helped provide a measure of false alarms that could be factored in with the number of each respondent's correct hits. This, in turn, allowed for the ability to analyze accuracy. A review of the data shows that, overall, the subjects in the experiment seem to have had remarkably few false alarms. In fact, most of the respondents had either 0 or 1 false alarms. There were a few outliers who reported 3 or 4 false alarms, but there were very few. However, Table 5-13 depicts an ANOVA performed on aroused-only groups and control groups based on mean false alarms.

**Table 5-13 - ANOVA of Aroused-Only vs. Control Group False Alarms**

ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	13.059	1	13.059	28.754	.000
Within Groups	46.326	102	.454		
Total	59.385	103			
MEANS					
	Aroused-only		Control		
	.7843		.0741		

While appearance, alone, seems to suggest that false alarms are not significant in this research, the ANOVA demonstrates a significance in difference of groups means at  $p=.000$  (See Table 5-13). This poses the question of what is a tolerable amount of false alarms to accept. Too many false alarms might result in complacency and a reduction in deception detection accuracy. Yet, depending on the importance of the information, a significant number might be tolerable. Also, it is possible that a considerable amount of productivity could be lost due to artifact users aroused suspicion of data veracity. In the course of this study, group task completion rates were also measured to determine if arousal does indeed influence productivity. However, since that does not directly affect the analysis of the hypothesis, it will be covered later in the post hoc analysis section of this chapter. The effects of deception detection training will be considered next.

## **The Effect of Training on Deception Detection Ability**

While experienced Personnel Specialists work the most with PC-III, downsizing initiatives and reconfigurations of squadron command sections have recently resulted in greater numbers of less experienced users entrusted to retrieve PC-III data and make decisions. With that in mind, another objective of this research is to determine if deception detection training would help improve user deception detection performance.

Johnson, et al., (1993) used a taxonomy of known deceptive practices to develop a training program designed to increase the deception capability of accounting auditors. Two of the three auditors they experimented with displayed improved deception detection ability when auditing fraudulent accounting reports. Furthermore, the respondents in the study were aware that fraud did indeed exist in the accounts. This research hopes to extend the work of Johnson and his colleagues by examining the influence of training (based on the taxonomy) on experienced groups of artifact users, inexperienced groups, aroused groups and unaroused groups. Thus the following hypothesis was posed:

### **H4: Deception Detection Training is positively related Deception Detection Ability.**

To test the hypothesis, a 30 minute training session was created based on the deception taxonomy (See Appendix F). Subsets of the Craftsman, Officer, and Apprentice groups were given the training. One subset of each group received the training a week prior to the experiment and was not aroused to the information manipulations in the PC-III database. Another subset of each group, the interaction group, received the training and arousing treatments immediately prior to the experiment.

User performances were recorded via a discrepancy recording sheet and loaded into data files.

Analysis of variance was conducted on via two avenues. First, the means of all trained groups (to included aroused groups) and all untrained groups were compared. Table 5-14 below depicts the findings of this ANOVA.

**Table 5-14 - ANOVA of all Trained Groups vs. all Untrained Groups**

ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	5.546	1	5.546	1.560	.213
Within Groups	721.752	203	3.555		
Total	727.298	204			
MEANS					
	Trained		Untrained		
	1.91		1.58		

It appears that the training made little difference in respondents' deception detection abilities. To gain a more specific understanding of the outcome of the training, the trained-only groups were compared to the control groups. A review of the data indicates that in the Officer and Craftsman groups the control groups actually performed better than the trained groups. An ANOVA of trained-only versus control groups was conducted to determine if this difference was significant, but it was not. The trained-only



Apprentice group performed only marginally better than their control group counterparts. Again, the training did not produce any significant improvement in user deception ability. Thus, Hypothesis 4 is not supported.

This outcome is unfortunate as it was hoped that deception detection training would yield increased ability, especially in less experienced users, to detect deception in the data. Reasons why the training was not effective will be covered in the discussion section of this chapter. Next, the final hypothesis will be examined.

### **The Interaction Effect**

Past research suggests that experience, arousal, and training are all factors that should influence deception detection ability in artifact users. With that in mind, it would seem likely that a group possessing all of these traits should demonstrate better performance than any other combination of the factors. This rationale leads to the following hypothesis:

**H5: User Experience in the Domain combined with Deception Detection Training and Arousal will provide greater positive influence on Deception Detection Ability than will Arousal, Deception Detection Training or a combination of the two.**

An ANOVA was conducted across all groups to determine if there were significant differences in their means. The results of this ANOVA are noted in Table 5-15 below. For the convenience of the reader, the group means of correct detections are provided in Table 5-16.

**Table 5-15 - ANOVA of all Groups**

ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	294.682	11	26.789	11.951	.000
Within Groups	432.616	193	2.242		
Total	727.298	204			

**Table 5-16 – Mean Scores of Correct Detections for all Groups**

	Control	Aroused	Trained	Interaction
Apprentice	0	1.41	0.33	2.94*
Officer	1.44	2.8	0.5	2.64
Craftsman	1.1	2.84	0.89	3.67

\* Includes 3 Outliers who reported considerable PC-III experience in other career fields

Clearly, the ANOVA helps to establish that there is a significant difference at the  $p=.000$  level. However, the hypothesis posits that one group, the Craftsman interaction group, should be better than all other groups with various combinations of treatments.

A review of the data in does indeed reveal that the Craftsman interaction groups produced a higher correct hit score mean ( $u = 3.67$ ) than any other group in the experiment. However, even with the ANOVA in Table 5-10, it remains to be seen whether the Craftsman interaction group was significantly better than the others. While an ANOVA can demonstrate that significant differences in means exist, Tukey's Honestly Significant Difference (HSD) test can indicate where the differences are. Therefore, a

Tukey's HSD was accomplished for all groups. Its results (at the .05 significance level) are noted in Table 5-17 below.

**Table 5-17 - Tukey's HSD of All Groups**

	Group	Mean Difference	Std. Error	Sig.
Craftsman Interaction Group vs.	Apprentice Control	3.8500*	0.494	0.000
	Apprentice Aroused	2.4382*	0.511	0.000
	Apprentice Trained	3.5167*	0.494	0.000
	Apprentice Interaction	0.9125	0.502	0.809
	Officer Control	2.4125*	0.502	0.000
	Officer Aroused	1.0500	0.511	0.656
	Officer Trained	3.3500*	0.502	0.000
	Officer Interaction	1.2071	0.522	0.467
	Craftsman Control	2.7548*	0.468	0.000
	Craftsman Aroused	1.0079	0.480	0.622
	Craftsman Trained	2.9553*	0.480	0.000
* Indicates Significance at the .05 level.				

According to the table, it appears the Craftsman Control Group performed significantly better than many of the other groups, but not all (better in 7 out of 11 cases). Those groups in which the treatment of arousal was involved (except for the Apprentice Aroused group) were not significantly different than the Craftsman Interaction group at the .05 level. This is not surprising given the findings regarding training and arousal

effects presented earlier in the chapter. The effect of arousal was quite strong and the effect of training was not. When aroused groups were compared to interaction groups, the difference was minimal. This finding underscores the earlier findings regarding training and arousal. While the Craftsman interaction groups did produce higher mean scores of correct detections, they were not high enough to provide statistical significance in some of the cases. Therefore, Hypothesis 5 received limited support. Further evaluation of the findings will be discussed later in the chapter after the following section on post hoc analysis.

### **Post Hoc Analysis**

One interesting observation made during the process of the experiment concerned the rate of task accomplishment by the respondents in the different groups. While the experiment was being conducted, it appeared that in aroused groups (both aroused-only and interaction groups), subjects were working somewhat slower than those in the other groups. Since all respondents turned in their scenario sheets, it turned out that counting the completed scenarios to obtain a quantitative measure of task completion was rather easy. This measure was added to the data files for possible future use. While a review of the data files suggests significant differences in groups means with regard to task completion rates, an ANOVA was performed to gain a better understanding. The results of that ANOVA are in Table 5-18 below.

**Table 5-18 - ANOVA of Task Completion Rates of Aroused vs. Non-aroused**

ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	505.853	1	505.853	23.781	.000
Within Groups	4296.750	202	21.271		
Total	4802.603	203			
MEANS					
	Aroused		Non-aroused		
	10.89		14.00		

When combined into groups of aroused and non-aroused, the ANOVA suggests, with a significance of  $p=.000$ , that arousal to the possibility of strategic information manipulation may affect the productivity of artifact users. In this experiment, aroused groups were less productive than non-aroused groups. This leads to the speculation that it may be possible to reduce productivity by merely arousing artifact users to the idea that the information produced may have been manipulated even when, in truth, the information is deception-free.

This finding may prove useful. From a deception standpoint, if deceivers wish to cripple their adversaries with little investment, all they may have to do is plant the idea that the adversary's information has been strategically manipulated. That may very well send the victim scurrying to find deception while his or her task completion or

productivity rate drops. A significant disturbance with minimal effort may be possible. While this observation and speculation is indeed fascinating, it requires further study before it can be further used. There is no theoretical basis to it, it was not hypothesized in this research project, and it is merely an interesting spin-off of the original study. Therefore, the remainder of the chapter will be devoted to discussing the results of the five hypotheses.

### **Discussion**

Results of the study are summarized in Table 5-19. Hypotheses 2 and 3, which tested the relationships between Experience in the Information Domain and Deception Detection Ability and Aroused and Deception Detection Ability, respectively, were both strongly supported. Hypotheses 1 and 4, were not supported, and Hypothesis 5 received limited support. This section discusses the possible explanations for these findings.

One of the main objectives of this research is to determine the effect truth bias has on a user's ability to detect deception in artifact produced information. Both the truth bias construct (McCornack and Parks, 1986) and Information Manipulation Theory (McCornack, 1992) suggests that humans can be deceived due to their truth bias toward another person. McCornack measured truth bias by measuring how many times a respondent could be deceived by a partner in a given situation (McCornack and Levine, 1992). The more times the respondent was deceived, the higher his or her truth bias.

This research project sought to learn if McCornack's theory and the truth bias construct could be extended to artifact-human relationships.

**Table 5-19- Summary of Findings**

<b>Hypothesis</b>	<b>Finding</b>
H1: Artifact truth bias is negatively related to deception detection ability.	<i>Not supported.</i> The PC-III Trust Scale not found to be an adequate predictor of truth bias.
H2: User experience in the information domain is positively related to user's Deception Detection Ability.	<i>Moderate to strong support.</i> Experience in the information domain is positively related to deception detection ability.
H3: Arousal (producing expectations of possible information manipulation) is positively related to Deception Detection Ability.	<i>Strongly supported.</i> Arousal is positively related to deception detection ability. It is also strong related to false detections.
H4: Deception Detection Training is positively related Deception Detection Ability.	<i>Not supported.</i> Deception detection training had minimal impact on deception detection ability
H5: User Experience in the Domain combined with Deception Detection Training and Arousal will provide greater positive influence on Deception Detection Ability than will Arousal, Deception Detection Training or a combination of the two.	<i>Limited Support.</i> While the group with experience, arousal and training did score higher than all other groups, differences with some groups not statistically significant.

To examine this issue, this research used a slightly modified version of the Rempel-Holmes Trust Scale to first obtain an independent measure of respondent truth bias toward an a particular artifact (PC-III) (Rempel and Holmes, 1991). Although pilot testing appeared promising, regression analysis determined that the scale explained only a small portion of the variance and was not a good predictor of deception detection ability.

An ANOVA comparing the deception detection ability of those with high truth bias scores to low truth bias scores supported the finding of the regression analysis.

A review of data suggests that one of the reasons for the disappointing results may be that the respondents had scores that clustered around 3, the neutral score. Thus, no matter what a respondent's demonstrated performance was, his or her truth bias tended to remain neutral. Another reason for the poor predictability of the scale may be due to the researcher's erroneous attempt to anthropomorphize PC-III. During post experiment interviews, many of the novice Personnel specialists maintained that they knew so little about PC-III that they could not form anything other than a neutral opinion of the system. The more experienced specialists revealed that they perceived PC-III to be nothing more than a tool. Additionally, they would point out that PC-III is only the communication channel, not the source of the data. As one respondent noted on her survey, "It's not PC-III I'm concerned with, it's the person on the other end." Thus, it appears the more experienced personnel have a tempered view of PC-III.

In an effort to increase the variance of the truth bias measurement, the median third of the sample was removed. The maneuver helped to counter the large number of neutral responses, and it was thought that such an action might improve the analysis of the influence of truth bias. Another ANOVA was accomplished on high and low truth bias scores, however, it offered little improvement to the original analysis.

The results of this finding suggest that truth bias and Information Manipulation Theory may not be appropriate tools to explain the phenomenon of artifact-human



relationships. It appears they cannot adequately capture the dynamic relationships between sender, information channel, receiver, and possibly, manipulator. Even when related measures of truth bias were used, significance was not obtained. It may be possible that the task itself, rather than a human trait or cognitive style is more of an influence on deception detection ability (Huber, 1987). Given the results of the post-experiment interviews, it might be interesting to examine an artifact like PC-III through an information channel perspective. Therefore, to answer the first research question, it does not appear that truth bias influences an individual's perception of artifact reliability in the same manner it influences perceptions of human truthfulness.

Hypotheses 2 through 5 were designed to help answer the question of whether or not factors such as arousal and deception detection training can be used to reduce human susceptibility to strategic information manipulation via artifacts. Hypothesis 2 considered the influence of user experience in the information domain as a means of increasing deception detection ability. Results of the experiment produced moderately strong support for this hypothesis. Since the researcher could observe the respondents at their tasks, the laboratory experiment proved to be an excellent approach to gain an understanding of the finding. First, unlike the novices, many of the experienced respondents appeared to have a pre-conceived notion of what information they needed to answer the question. If the data did not appear as they expected it to, they became suspicious. Second, the experienced respondents were better at organizing the data. They would often draw charts and matrices on their scenario sheets so they could better

compare information across records. Finally, the experienced respondents focused directly on the information they needed. They knew where it was on the screen and they went to it discarding unnecessary information. Understandably, the novices did not display these tactics. Thus, it is not surprising that experienced respondents did perform better than their novice counterparts.

Hypothesis 3 examined the influence of arousal on deception detection ability. This hypothesis received very strong support. This is not surprising given the findings of Klein and her colleagues (Klein, et al, 1993). When users are tasked to find deceptive data, they can do it. However, Air Force Personnel specialists, like many others in information intense occupations, are often required to work under considerable time pressure. Such was the case of the respondents in the experiment. They were given 90 minutes to complete the 20 scenarios. Those groups that did not receive the arousal treatment focused on completing the task while those that were aroused focused on finding the deceptive data. A post hoc analysis demonstrated that the task completion rate of those respondents that were aroused was significantly less than that of the respondents who were not aroused. This suggests that even the belief of existence of deceptive data could significantly reduce user productivity. Unfortunately attempts to measure respondents' vigilance decrement levels were unsuccessful.

Hypothesis 4 attempted to examine if respondents' deception detection ability could be improved. This hypothesis was not supported. A training program was developed based on a taxonomy of deceptive practices (Johnson, et al., 1993). This

training was administered to some groups weeks before the experiment took place (to avoid arousal) and other groups at the time of experiment (to interact with arousal). There are a number of possible explanations for the lack of support. First, the effectiveness of this training program was not assessed. While the students did listen well to the instruction and seemed to enjoy it, no evidence was available indicating the content was retrained. Second, the respondents were in the middle of their Air Force training. Due to shrinking military budgets and the merging of career fields, instructors are forced to teach and students are forced to learn more information in a shorter period of time. Courses that used to be 8 weeks long in the mid-1980s are now 5 weeks long. While the training schools still provide a vital service at indoctrinating new members, much of what an airman learns is on-the-job (OJT). Third, it appeared that when the novices were in the deception detection training, they did not have an adequate frame of reference to adequately understand the deception methods. Some students simply could not comprehend some of the tactics. Fourth, in the case of the interaction groups, respondents reported in the debriefing that they were aware of the possible deceptions, but they simply forgot the training and used their own methods of detection. As a result, the interaction groups proved to be only slightly better than the aroused groups. Finally, it is possible that the training method was inappropriate. Respondents were given the training in the same manner as they received all of their other instruction. It is possible that training-on-demand might be a more appropriate method for a task such as deception detection. In this study, respondents were primarily tasked to complete scenarios, not to

detect deceptive information. Had the training approach allow them to receive training at the point they first suspected a deception rather than at a time somewhat earlier than the deceptive event, the outcome may have been different.

Hypothesis 5 maintained that the experienced group that was aroused and received deception detection training (the Craftsman Interaction group) would performance better than any other group combination. The group did have a higher mean score than any other group in study. However, a Tukey's HSD demonstrated, at  $p = .05$ , that the Craftsmen Interaction group performed significantly better than only 7 of 11 groups. The above discussions regarding the strength of the arousal treatment and the weakness of the training treatment provided adequate explanation for this finding.

In summary, truth bias and Information Manipulation Theory do not appear to be appropriate means of understanding strategic information manipulation via artifact channels. Respondents given time intensive and information intensive tasks will overlook many deceptions in an effort to achieve task completion. Experience in the information domain and arousal to the fact the strategic information manipulation has taken place can lead to increased deception detection ability. However, for those in the aroused groups, the increased detection ability came at the cost of productivity. Training to increase deception detection ability proved to have an insignificant effect. Even though experienced groups with training and arousal scored the highest overall, it was arousal that proved to play the greatest role in increasing deception detection performance.

## **CHAPTER 6**

### **CONCLUSION**

This research was motivated by the increasing role information artifacts are playing in decision making and by the opportunities for strategic information manipulation. Since computer-based preventive measures for information security have demonstrated a lack of effectiveness, the issue of artifact user ability to detect deception requires examination. This research is an attempt to better understand human deception detection in artifact-produced information. Its goal is twofold. First, by examining user behavior through a truth bias lens, it was hoped that more could be learned about the trust humans place in the artifacts they use. Second, by borrowing from the literature on individuals' abilities to detect deception by significant others, factors influencing such abilities were investigated. These two avenues were then used for the ultimate objective of determining how to improve users' ability to detect deception in artifact-produced information. Some of the key findings are discussed below.

## Summary of Findings

One key goal of this research was to determine if current theory on truth bias and information manipulation in human-to-human relationships could be adapted to artifact/user relationships. In order to examine this, respondents answered a survey instrument design to elicit their truth bias level toward a familiar artifact. Like the supporting theory, the survey was taken from research on human-to-human relationships and adapted for this research endeavor. Unfortunately, that measurement of truth bias did not prove to be a good predictor of deception detection ability. When combined with other supporting measures of truth bias, little improvement was noted. The aggregate reports of the respondents indicated a somewhat neutral opinion of the artifact. Novice respondents reported unfamiliarity with the artifact as the reason for their neutrality. More experienced respondents cited their philosophy that the artifact was more of an information medium than a source. Because of this finding, this research could not support theories based on truth bias such as Information Manipulation Theory (McCornack, 1992) and Interpersonal Deception Theory (Buller and Burgoon, 1996) as means for explaining human trust in artifacts.

Another facet of this research sought to learn how deception detection performance could be enhanced. Signal detection theory was used to explain this phenomenon. Users were divided into groups based on unrelated classes they were attending. These groups were then designated as control, aroused, trained (or trained-

only) and interaction. The treatment groups were examined based on the factors of experience in the domain (information domain), arousal, and training.

It was hypothesized that those respondents who were more experienced in the information domain would have better deception detection abilities. This hypothesis was supported. More experienced respondents did perform significantly better in the experiment than did the novices. This provides support for Signal Detection Theory (Davies and Tune, 1969) as experienced respondents proved to be better at differentiating deceptive signals from background noise. Interestingly, one of the groups, the Officers groups, reported some experience in the field. While they did seem to perform better than the novices and not as well as the more experienced respondents, neither difference was found to be statistically significant. However, this finding may help to answer the question of how much experience in the information domain is needed for artifact users to better identify the signals of deception.

Another hypothesis examined the influence of arousal on deception detection ability. This hypothesis was strongly supported. Respondents who were aroused to the fact that the data in the artifact they were using contained deceptions demonstrated significantly greater detection abilities than the control group. This finding also provided support for signal detection theory (Davies and Tune, 1969). Aroused respondents focused more of their energy toward identifying deceptive signals than did the non-aroused groups. However, they did so at a cost to productivity. In a post hoc analysis, aroused groups were compared to non-aroused groups with respect to their task

completion rate. The aroused groups were found to be significantly less productive. This begs the question: What impact does the perception of deception have on task performance?

A further hypothesis focused on the influence of deception detection training on deception detection ability. Using a taxonomy for deceptive practices developed by Johnson, et al., (1993), a training program was developed and administered to some groups of respondents. Unfortunately, the training did not help to improve respondents' deception detection abilities and the hypothesis was not supported. It is believed that novice groups' lack of experience in the domain prevents the respondents from having an adequate baseline from which to form an understanding of how the training applies. Training does not appear to be an adequate substitute for experience. In the experienced groups, respondents reported using their own deception detection methods (if any). Thus, the training program proved ineffective.

A final hypothesis suggested that an experienced group that was trained and aroused would outperform any other possible combination of groups. The data supported this hypothesis, but analysis demonstrated that group differences were significant only 7 of 11 cases. Earlier findings showing the strength of arousal and the weakness of the training suggest little interaction effect when the two are combined. The findings regarding the lack of significant difference in the groups with some experience and the groups with greater experience also support this outcome.



In the end, experience in the information domain and arousal proved to be the factors that most significantly improved user ability to detection deception in artifact produced information. However, the arousal treatment also led to a decrease in task productivity. The findings of this research have both academic and managerial implications. These will be addressed in the next two sections.

### **Academic Implications**

The findings noted above have a number of implications for future research. First, alternative approaches toward understanding the truth bias construct may produce more positive results. This research made an attempt at anthropomorphizing an artifact by examining an artifact/human relationship. This proved to be ineffective. Many of the subjects in the experiment maintained that the artifact was nothing more than an information medium or channel. Thus, attempting to measure their attitude toward its veracity produced a measure that was ineffective at predicting artifact user deception detection ability.

Second, if the measure of truth bias used was adequate, it is possible that truth bias may not be a good predictor of deception detection ability. Those respondents reporting low truth bias did just as poorly as those reporting higher measures of the construct. Many of the deceptions included in the experiment were very blatant, even to the untrained eye. A person with even the smallest amount of experience in the domain

(i.e., an Apprentice student) should easily recognize some of the deceptions. Yet, many subjects succumbed to time pressures and a desire to be finished thereby disregarding warnings of problems with the data. Thus, truth bias may be only one of many pieces of the puzzle. It is possible that time constraints, political context, the criticality of the task, the ease of access to the information, and ease of use of the system may have an influence on deception detection ability. In the laboratory experiment, the respondent did face some time constraints and had to rush to complete their work. This helped to simulate real world events, but, it was not the same as the time pressure they face in the real world. Since no consequences were realized by the respondents for failing to complete the task, they may have viewed it as having a low risk even when they knew the information was compromised. Further, PC-III is often the only source of information or the only easy source of information. Respondents may have chosen access over accuracy (O'Reilly, 1982). In sum, there appears to be many influences on deception detection ability.

Third, the relative poor performance of those in the trained groups should be examined. While the respondents were attentive and involved during the training, training did not seem to have much of an effect on their deception detection abilities. Perhaps differences in their individual cognitive styles were a factor influencing their deception detection behaviors. Zmud, in his review of the empirical literature, noted how "...individual differences believed most relevant to MIS success are grouped into three classes: cognitive style, personality, and demographic/situational variables" (1979,

p 967). This appears to apply to deception detection success as well. A casual review of respondent worksheets revealed that many of the more experienced subjects copied much of the information they needed off the PC-III screen and organized it so as to compare with other data. While not analyzed statistically, it appears that those respondents who organized the information available to them did better at detecting the deceptions than those who attempted to answer the scenario by merely looking at the screen. This was apparent in nearly all of the groups. Personality differences such as willingness to participate and situational differences such as level of task knowledge seemed to influence the outcome as well. The latter observation was evidenced in the findings regarding Hypothesis 2. Also, the Craftsman students brought with them a tacit understanding of PC-III and seemed to rely more on what they knew about the system (e.g., methods of double-checking the data that were unknown to the researcher) than on deception detection techniques taught to them. It is also possible that the deception detection training had to compete with respondents' attention to other training (testable training) or was an inappropriate method to use for teaching deception detection skills. In sum, the training provided to the respondents may not have been adequate enough to influence their information processing behaviors.

Finally, the method used for data collection has some implications. While this research approach was labeled a laboratory experiment with supplemental survey instrument, other forms of information collection were exploited as well. After subjects were debriefed, there were opportunities to get their feedback. Many subjects had stories

to tell about their experiences with PC-III or with computer security problems they have encountered at their bases. In another case, the researcher was asked to supervise a classroom of Apprentice respondents (after the experiment was completed) when their instructor was summoned away. Again, there were more stories and more points of view.

The point is that even though planned methods of data collection are of primary importance, much can be learned from emergent opportunities. For example, the Apprentice group respondents demonstrated a rather poor performance at detecting deceptive information in PC-III. Near the end of the experiment, the researcher was asked by the supervisor of the training development staff to review and comment (as a favor to the supervisor) on some feedback surveys received from the field. Many of the surveys noted that airmen were going into the field without adequate PC-III training even though they complete their courses<sup>1</sup>. This opportunity helped the researcher gain a better understanding as to why there were low performances during the experiment.

### **Management Implications**

This research endeavor also provides some implications for managers as well. In fact, the findings presented here probably offer more to the applied world than they do to that of the academic. One finding that should be of interest to managers in all

---

<sup>1</sup> At the end of the experiment, course supervisors and training development staff asked they could continue to use the scenarios as part of their PC-III curriculum.

organizations that use information artifacts is the low overall performance of the respondents with regard to identifying deceptive data in the information systems they use. Even the seasoned Personnel specialists were unable to identify many of the discrepancies. Some of these people reported spending over 50 percent of their days working with PC-III. The overall mean correct detection rate was a mere 1.74 (See Table 5-15 for means of individual groups) for an 11.6 percent success rate. Even the best group, the Craftsman Interaction group produced an average of 3.67 correct detections. That is a 24.5 percent success rate. If this experiment were a real world event (as it easily could be), the artifact users' decision making quality could be seriously jeopardized. It is important to note, however, that experience in the domain and arousal, significantly improve deception detection performance. Experience in the information domain appears to be without substitute. How much experience is necessary remains a subject for future research. Arousal does improve ability to detect, but it comes at a cost.

A post hoc analysis demonstrated that when subjects were aroused, their task productivity decreased significantly. When respondents learned that the data they were using was flawed, they decreased their emphasis on completing the scenarios that they were assigned and began to search exclusively for errors. Aroused subjects also found more false alarms than did their not aroused counterparts. The implication here is that not only is decision-making quality reduced by deceptive information, but productivity may be decreased as well.

Another implication for managers concerns the design of information systems. This research raises two concerns. First, there is the concern of over-reliance on the artifacts' programmed abilities to foil deceptive practices. When the PSMs were first approached about the experiment, they explained that it would be difficult to accomplish as PC-III has many system edits to prevent data tampering. However, all of the manipulations created for the scenarios were produced within the confines of the system edits. Even the PSMs were surprised how much information manipulation could take place. This finding suggests that managers place too much reliance on computer based approaches to data protection.

Second, in post-experiment interviews, many respondents explained that they found it difficult and time consuming to compare data items in an effort to detect deceptions because they had to scroll through many screens to do so. This would suggest to information system designers that certain types of system designs might prove to be more useful for deception detection endeavors while other might inhibit them.

In summary, the research holds considerable implications for managers. In this day and age of artifact dependency in nearly every industry, it clearly denotes the vulnerabilities of such reliance. Strategic information manipulation not only affects decision-making, it has potential ramifications for productivity and system design as well. The next sections will consider some of the strengths and weaknesses of the research.

## Strengths

The main strength of this research lies in the method by which it was accomplished. The laboratory experiment allowed for many opportunities that other methods could not accommodate. First, the respondents were individuals working with an artifact they either did work with on a daily basis or would be working on it soon (i.e., the Apprentice group respondents). Unlike laboratory studies where respondents and tasks often must simulate real world types of people and events, this research used respondents doing tasks that closely mirrored their daily responsibilities. Second, this experiment used a specific information artifact that was known to the respondents and used for tasks like those they were assigned to accomplish. Thus, the element of realism was quite high. It was so high that course instructors asked for copies of the task scenarios so that they might provide more realistic training to their students.

The third strength lies in the control of the experiment. Due to the nature of the research setting, the respondents had very little leeway to do anything other than the assigned task. The respondents were rather homogeneous within their group types, and distractions could be held to a minimum. Further, the identification codes on each of the data collection devices allowed for their tight control. Thus, control was rather tight.

The final strength was the opportunities for extra data collection this method offered. Before, during, and after the experiment, the respondents could be observed in their natural setting. Follow-up interviews both with the groups and individuals allowed

for clarification of the findings. Also, because the researcher was present at all times post hoc observations were easily accomplished.

### **Limitations**

While a number of strengths were highlighted in the last section, this study is not without its limitations. One of the key concerns may be the performance of the scale used to measure truth bias. While this scale has a proven track record in human-to-human relationships, it may not be fitting to apply it to artifact/human relationships to obtain a measure of truth bias. However, previous research on human-to-human relationships operationalized truth bias by measuring the number of truthful judgments made by subjects (McCornack and Parks, 1986). Research attempts to replicate this approach did not provide support (Buller, 1988; Stiff, et al., 1989). This research attempts to measure, first, users' attitudes regarding the reliability of a familiar artifact (i.e., their truth bias) and then measure their detection ability. Thus, it provides for two truly independent measures. Correlations with two other scales measuring users' attitudes toward computers in general and toward PC-III data quality were found to be significant. Both of these scales contributed to the understanding of user truth bias toward the artifact, but neither proved to increase predictability of detection accuracy.

Another possible limitation involves the development and use of the deception taxonomy training materials. While Johnson, et al., (1993) provided a detailed



description of their taxonomy and methods of identifying when deception approaches in the taxonomy were used, their explanation of their training program was limited. Therefore, the researcher had to rely on his own personal experience while developing the lesson plan used for this research. It is possible that if the original training program was used, the results may have been different. However, every attempt was made to ensure the trained respondents understood the taxonomy and the various approaches. The only way to confidently assume the respondents retained the information is to measure their taxonomy knowledge. Due to restrictions at the research site, this could not be accomplished.

A final limitation of this study was the restrained amount of pilot testing accomplished. Due to time restraints and limited sample size, pilot testing was not as robust as desired. Had more pilot testing been conducted, it is possible that the poor performance of the truth bias measure as a predictor of detection ability could have been identified. However, the pilot testing was invaluable for reliability and content validity analysis. It also helped to ensure the smooth flow of data collection and respondent attitude toward the research endeavor. Opportunities for future research are provided in the next section.

## **Opportunities for Future Research**

There are numerous opportunities for future research in this arena. While signal detection theory appears to adequately explain the factors influencing deception detection performance, a better theoretical basis for understanding artifact/human relationship is needed. Existing theories of human-to-human relationships do not appear to adapt to this phenomenon. The differences in the relationships may be too great. It is possible that viewing the phenomenon as a medium rather than a source of information might prove to be a better lens.

Future research might also investigate why there was little variance in truth bias measurement between respondents. It is possible that the lack of variance in the truth bias measurement was due to the system design. Therefore, a study to determine if different types of systems and different types of system designs influence user truth bias measurements might be in order. It is also possible that the respondents in this study did not understand the reality of how fragile the system can be and made their judgements based on their beliefs about computers in general. Also, while the laboratory experiment was a close match to reality, the lack of true time pressure and political context (respondents face no consequences for failing to finish or for incorrect answers) might have affected the truth bias measurement outcome. These concerns should be examined in future research.

Another interesting area of research comes from the post hoc findings of this project. Aroused respondents exhibited a significant decrease in productivity. When they learned of the possible manipulation of the information, they began to focus on finding the deceptions and reduced their efforts to complete the task. It would be interesting to determine if merely the suggestion of deception produces the same results. Further, it would be useful to determine just how long the arousal treatment would be effective.

The development of a training program to improve deception detection ability would be a valuable contribution to an information-intensive organization. This study learned that developing such training is a challenging endeavor. Further, the study demonstrated that experience has a positive influence on deception detection ability. In this day and age of downsizing and flattening of organization hierarchies, it is often the experienced personnel that are removed. As such, it would be interesting to learn if training for deception detection could somehow make up the difference. While this was not a primary objective, this study found evidence to the contrary. It would also be interesting to determine how much if experience is necessary to produce adequate detection ability.

Like most research, this study surfaces as many or more questions than it answers. Why are users vulnerable to deceptions in artifact produced information? How obvious must deceptions be to promote identification? Can users ever be trained to satisfactorily detect deceptions in artifact-produced information? Zmud (1990)

offered a number of propositions to explain the strategic information manipulation phenomenon. This study made an exploratory attempt at investigating some of those propositions. Closing comments are provided in the final section below.

### **Summary**

With such a strong reliance on artifacts to produce information for decision making, the time is right to consider the capability of individuals (who use artifact-produced information in decision making) to detect when strategic manipulation of their information occurred. The literature shows computer-based methods of deception prevention and detection are not foolproof. At the same time, theories from human-to-human communication literature and a taxonomy of deceptive practice from the accounting literature offer a means to possibly improve human ability to detect artifact-based deception. The results of this study demonstrate that user ability to detect deceptive information in a familiar artifact is limited. Further, experience in the domain and arousal can improve detection performance, aroused suspicion of information veracity can reduce productivity, and development of a training program to increase user detection ability can be difficult. Clearly, opportunities for further research in this area abound as reliance on artifact-produced information continues to grow.

**APPENDIX A**  
**EXPERIMENT TASK SCENARIOS**

### Scenario 1

Two airmen working in the same section want to take a lunch time class at the education office in pursuit of their Bachelor's degree. Because of manning shortages, they cannot both go. Their names and SSANs are provided below. Their supervisor decided that if one of them already had a degree the other would be allowed to take the class. Unfortunately, neither of the airmen are currently available to ask. Review the airmens' records. Does either of them already have a degree? If so, which one? \_\_\_\_\_  
(Enlisted Qualification Data)

Gray, Christian A.	123565450
Greene, Hollitte D. IV	123307024

### Scenario 2

Four airmen are up for below-the-zone promotion. Review their records and ensure they each have at least two years time in service, a decoration, and at least a 4 EPR. Run an inquiry on their time-in-service, decorations, and last EPR. Their names and SSANs are provided below. Are all of the airmen eligible for promotion. (Circle one) Yes. No.  
(Airman Service Dates, Awards and Decs, EPR Info)

Ahlberg, Keri L.	123067580
Balakit, Macario, B. Jr.	123035446
Chaptman, Joseph E. Jr.	123476885
Dimauro, Patrick, M.	123028649

### Scenario 3

The records of four officers must be reviewed for possible reassignment. Review the records and determine which officer, based on his/her date arrive station, duty title, and tour status is most eligible for the assignment. Conduct an inquiry and review the officers' date arrived station, duty title, and tour status. The names and SSANs are provided below. Who should be up for the assignment? (Circle one) A, B, C, D  
(Duty Assignment Data, p2)

Bentley, Terry R.	123409960
Birch, David L.	123371503
Chihuahua, Taylor	403449417
Keating, Matthew, M.	123277526

#### Scenario 4

Four officers are being considered to attend Squadron Officer School in residence. Their names and SSANs are provided below. Review the officers' GRADE, TAFMCD, AFSC, and unit to determine the best selectee for the school. Typically, the highest ranking officer goes. (Circle one) A B C D (OPR Info)

Fisher, William L.	123575680
Halsrud, Clyde E.	123481702
Marcellus, Wallace	484549310

#### Scenario 5

Four MSgts on your base have recently been selected for promotion to SMSgt. Your Chief, MPF wants to run a quality control check on all promotions and wants you to review the MSgts' records to look for commonality. He/She wants to learn if there is anything about these MSgts' records that might help other MSgts meeting future promotion boards. A list of four MSgts and their SSANs is provided below. Review the selectees last EPR, Decorations, and Degree levels. Do you see any commonality? (Circle one) Yes. No. (EPR Info, Awards and Decs, Enlisted Qualification Data)

Heller, Douglas, M.	165541895
Hoek, Ren	123245802
Joyner, Lance L. Jr.	123238964
Krajicek, Dayton C.	123512600

#### Scenario 6

Your commander wants to review all of the members of the squadron on the weight management program (WMP). She wishes to learn if those members have shown unsatisfactory performance in other areas as well. For the list provided below, run an inquiry on the members WMP code, check to see if they have any open unfavorable information files (UIF), and pull the score for their last EPR. Are there members with more problems than just weight management (Circle one) Yes. No. (EPR Info)

Angel, Vincent R.	123456474
Aster, Sylvester, E.	123266839
Ballard, Mary B.	123428256
Bauman, Dan, L.	123395521

### Scenario 7

A SSgt in your squadron wants to re-enlist. Your commander is new to the unit and wishes to know if he (the SSgt) is eligible to reenlist. His name and SSAN is provided below. Is the SSgt eligible for re-enlistment? (Reenlistment/Separation Data)

Butts, Larry A.	123452270
-----------------	-----------

### Scenario 8

Recently, there has been a change in area code for some of the members of your unit. On a recent recall, it was learned that four of the members failed to get their phone numbers changed in the sytem. Pull the phone numbers of those four members and check to ensure the phone numbers are correct. The area code for each should be: 228 Do all of the members now have correct phone numbers? (Circle one) Yes. No. (Individual's Data)

Berry, Michael, S. Jr.	123272801
Bessert, Leona, M.	123379045
Boston, Ambrose, D. Jr.	123424064
Bova, Katherine, M.	123099748

### Scenario 9

The first sergeant is doing a dependent care review and has some concerns regarding the four members listed below. He wants to know the number of dependents each of these members have including the number of adult and minor dependents. Please note the number of dependents for each member. (Individual's Data)

Bowling, Kathy A.	123267590
Brinsfield, Michael A.	123238235
Brundidge, Marvin C.	123549902
Carter, Anthony, W.	482460473

Member	Number of Dependents	Adult	Minor
--------	----------------------	-------	-------



### Scenario 10

A Training Group commander wants to select a Top Tech team. All candidates must have at least one year time on station, must have a Personnel AFSC or Communications AFSC, and must have a "T" prefix. Do all candidates meet the criteria? (Circle one) Yes. No. (Duty Assignment Info, p2)

Carpet, Adam W.	123560733
Cash Naomi	123425067
Chihuahua, Taylor	403449417
Coakley, Howard E.	123280484

### Scenario 11

A member of your squadron has an Article 15s. Check the disposition dates to determine when the UIF will close out. The name and SSAN are provided below. When will it close out first?  
(EPR Info)

Brown, Anthony	123423889
----------------	-----------

### Scenario 12

A Wing Commander wants to ensure consistency in duty titles (i.e. all squadron commanders have duty titles as squadron commanders) For the following members, run and inquiry on their duty titles and supervisors duty title. Are they pretty much consistent? (Circle one) Yes. No.  
(OPR Info)

Halsrud, Clyde E.	123481702
Brundidge, Marvin C.	123549902
Amato, Gerard, A.	123426962
Fisher, William, K.	123575680

### Scenario 13

TSgt Anderson came to you complaining that none of her dependents seem to have Delta Dental coverage. Use PC-III to see if TSgt Anderson's even has dependents. How many, if any, are noted in the system? \_\_\_\_\_ (Individual's Data)

Anderson, Darlene R.	123315722
----------------------	-----------

### Scenario 14

The MPF commander wants to review the last four winners of the Wing NCO of the Quarter award to look for trends. Their names and SSANS are provided below. Run an inquiry on their AFSCs and Duty Titles. Do you see any trends developing (i.e. all with the same AFSC or Duty Title? (Circle one) Yes. No. (Duty Assignment Data)

Aster, Sylvester, E.	123266839
Angel, Vincent R.	123456474
Ballard, Mary B.	123428256
Bauman, Dan L.	123395521

### Scenario 15

Four airmen are being considered for a TDY. Their unit commander wants to select the airman with the most time on station for the job. Their names and SSANs are provided below. Which airmen should be the one to go TDY. (Duty Assignment Data, p2)

Achille, Marie M.	123593620
Manchester, Bertha L.	123551911
Bisbee, Thomas G.	123016562
Bratton, Jacob A.	123435231

### Scenario 16

A Wing commander has learned that the next 4 personnel who leave the base will not be replaced for 6 months. Candidates A thru D below are possible losses. Pull the duty title, time on station information, and tour status for each. Who will be the first to leave. (Duty Assignment Data, p2)

Charles Haddon Spurgeon	123347385
Anderson, Darlene R.	123315722
Amato, Gerard, A.	123426962
David, Claude, A.	123416927

### Scenario 17

Capt Halsrud is a flight commander of a training squadron. This is important to him because he believes this job will get him a "C" prefix on his AFSC which will show in his record that he has had some command time. Is he in a duty position that will allow him to have an "C" prefix. (Duty Assignment Data, p2)

Halsrud, Clyde E.	123481702
-------------------	-----------

### Scenario 18

The first sergeant of your unit heard that a few people living in the dorms were "ghosting." That is, they have assigned dorm rooms, but they choose to spend their own money and live off-base. Often people who ghost change their address so their pay statements and other AF correspondence comes to their off base address. Check the addresses of these personnel to determine if they still maintain dorm addresses. Do any have off-base addresses? (Circle one) Yes. No. (Individual's Info)

Gretta, James S.	123268867
Griffin, Donald W.	123300604
Boykin, Bobbie, G. Jr.	123559859

### Scenario 19

For NCOs have been selected to attend the NCO Academy in residence. Their names and SSANs are provided below. Your commander believes one of the NCOs is overweight and may be on the weight management program (WMP). Use PC-III to determine if any of these NCO is on the WMP. If any, write the name(s) on the line below. (Awards and Decs, EPR Info)

---

Lythgoe, Clare J.	123528040
Marbut, Elizabeth, D.	123328687
Mathis, Gary W.	123424048

### Scenario 20

A new squadron commander (Lt Col Whitley - 123221342), wanted to know whose performance reports (EPRs, OPRs,) he rated. List the names, grades, and duty titles of the personnel he rates in the blank area to the right of the steps to produce the report listed below.

To answer this question: (Note + = transmit)

1. Go to reports and rips in the opening menu+
2. Select reports+
3. Select Performance Reports+
4. Combined...+
5. Rater's Subordinate...+
6. Enter Supervisor's SSAN+
7. F3 (Back to main menu)
8. Office Automation...+
9. Products+
10. Select Report+
11. View and Pg Dn

**APPENDIX B**

**INFORMATION MANIPULATION DESCRIPTIONS**

### Scenario 1

Two airmen working in the same section want to take a lunch time class at the education office in pursuit of their Bachelor's degree. Because of manning shortages, they cannot both go. Their names and SSANs are provided below. Their supervisor decided that if one of them already had a degree the other would be allowed to take the class. Unfortunately, neither of the airmen is currently available to ask. Review the airmens' records. Does either of them already have a degree? If so, which one? \_\_\_\_\_  
(Enlisted Qualification Data)

Gray, Christian A.	123565450
Greene, Hollitte D. IV	123307024

#### Description of Deception

This is a *clean* scenario in that there is no deceptive data involved. The respondents merely have to look up under Enlisted Qualification data, the education records of each of the two members. When they do, they will find that Greene already has a degree.

### Scenario 2

Four airmen are up for below-the-zone promotion. Review their records and ensure they each have at least two years time in service, a decoration, and at least a 4 EPR. Run an inquiry on their time-in-service, decorations, and last EPR. Their names and SSANs are provided below. Are all of the airmen eligible for promotion. (Circle one) Yes. No.  
(Airman Service Dates, Awards and Decs, EPR Info)

Ahlberg, Keri L.	123067580
Balakit, Macario, B. Jr.	123035446
Chaptman, Joseph E. Jr.	123476885
Dimauro, Patrick, M.	123028649

#### Description of Deception

Nearly all airmen entering the Air Force learn early about below-the-zone (BTZ) promotions. Airmen are eligible for this advancement when they attain the rank of Airman First Class (a.k.a. A1C). If selected for BTZ promotion, they may 'pin on' the

rank of Senior Airmen (SrA) six months earlier than their peers. Often commanders review the records of their eligible airmen to help determine the few to be selected for this opportunity. Ensure they have adequate time in service, checking to see if they have decorations, and review the ratings of candidates' Enlisted Performance Reports (EPRs) is a part of the selection process. Personnel specialists are often required to collect and summarize this data for the commanders, and highlight any information that may look out of the ordinary. In this scenario, Balakit has three Meritorious Service Medals (MSMs) in his records. This is not possible for a member of his rank. An MSM is a difficult decoration to achieve and usually requires years of service. In the taxonomy of deceptive practices this might be considered "inventing." (Johnson et al, 1993). This should be a fairly easy catch for most subjects.

### Scenario 3

The records of four officers must be reviewed for possible reassignment. Review the records and determine which officer, based on his/her date arrive station, duty title, and tour status is most eligible for the assignment. Conduct an inquiry and review the officers' date arrived station, duty title, and tour status. The names and SSANs are provided below. Who should be up for the assignment? (Circle one) A, B, C, D (Duty Assignment Data, p2)

Bentley, Terry R.	123409960
Birch, David L.	123371503
Chihuahua, Taylor	403449417
Keating, Matthew, M.	123277526

### Description of Deception

This deception is a somewhat more difficult to detect. All applicable fields are found in the Duty Assignment Data menu on page 2. One of the key fields in this menu is the Air Force Specialty Code (AFSC). This is a 4 digit alpha-numeric code that tells what career fields the officers are in. Include with the AFSC is often a prefix indicating that the individual is a some special duty assignment. For instance, a "T" prefix indicates the officer is in an instructor's position. A "C" prefix indicates a command position. In this scenario, one of the officers has a "T" prefix indicating that he is an instructor. However, he also has a duty title of "Student." In the Air Force, students are not considered for assignments. Because the duty title information was modified to suggest an incorrect decision, this form of deception would be called "mimicking" in the taxonomy. All of the subjects understand the AFSCs, but only those with experience in the field (or possibly another Air Force field) would understand the significance of the prefixes. Those respondents should note this discrepancy.

#### Scenario 4

Four officers are being considered to attend Squadron Officer School in residence. Their names and SSANs are provided below. Review the officers' GRADE, TAFMCD, AFSC, and unit to determine the best selectee for the school. Typically, the highest ranking officer goes. (Circle one) A B C D (OPR Info)

Fisher, William L.	123575680
Halsrud, Clyde E.	123481702
Marcellus, Wallace	484549310

#### Description of Deception

Squadron Officer School (SOS) is a form of professional military education in the Air Force. Assignments to attend SOS in residence (rather than complete by correspondence) are highly coveted and can make a difference at promotion boards for young officers. In this scenario, one of the officers had their information education information deleted (masking). In the Air Force, an officer must have at least a Bachelor's Degree. If this information is not in the PC-III system, the situation should be highly suspect. This scenario did not tell the subjects to look at officer education, but the information is located on the same screen with all of the other information that requires review for the decision. If a respondent sees that an officer has no education, he or she may not highlight the officer for selection even though he is the most qualified based on the criteria.

#### Scenario 5

Four MSgts on your base have recently been selected for promotion to SMSgt. Your Chief, MPF wants to run a quality control check on all promotions and wants you to review the MSgts' records to look for commonality. He/She wants to learn if there is anything about these MSgts' records that might help other MSgts meeting future promotion boards. A list of four MSgts and their SSANs is provided below. Review the selectees last EPR, Decorations, and Degree levels. Do you see any commonality? (Circle one) Yes. No. (EPR Info, Awards and Decs, Enlisted Qualification Data)

Heller, Douglas, M.	165541895
Hoek, Ren	123245802
Joyner, Lance L. Jr.	123238964
Krajicek, Dayton C.	123512600



### Description of Deception

As the scenario states, all of the Master Sergeants have been recently selected for promotion to Senior Msgt. The respondents must review the records of the selectees and determine if they have commonality that the Chief, Military Personnel Flight may be able to provide to other MSgts coming up for promotion. In this case, however, one of the selectees has a significantly low Enlisted Performance Report (EPR). On the EPR scale, a rating of 5 is high and a rating of 1 is low. The EPR system is somewhat inflated. For those at the MSgt grade of rank, anything less than a 5 is undesirable and would likely prevent a person from being promoted. In this scenario, one of the selectees has a 3 EPR. This would certainly prevent promotion. The respondents should pick up on this and flag it for investigation. This might be considered as "decoying" in the taxonomy. Airmen learn fairly early in their careers about the performance report system. Personnel specialist in all groups of this study received training on the EPR system as part of their course curriculum. However, since the information is new to the less seasoned troops, this is probably a moderately difficult catch for them.

### **Scenario 6**

Your commander wants to review all of the members of the squadron on the weight management program (WMP). She wishes to learn if those members have shown unsatisfactory performance in other areas as well. For the list provided below, run an inquiry on the members WMP code, check to see if they have any open unfavorable information files (UIF), and pull the score for their last EPR. Are there members with more problems than just weight management (Circle one) Yes. No. (EPR Info)

Angel, Vincent R.	123456474
Aster, Sylvester, E.	123266839
Ballard, Mary B.	123428256
Bauman, Dan, L.	123395521

### Description of Deception

In this scenario some of the airmen are not even on the WMP. It is possible for the respondents to overlook that fact and simply look for other unfavorable information even though the information is on the same screen. Air Force members on the WMP face certain restrictions such as not being authorized to get an assignment, go to professional military education in residence, go to technical training programs, or go on other temporary duty assignments (TDY's). Thus, it would be detrimental for a member who was

not truly on the WMP to have it in his or her record that he or she is in program. Further, if member is supposed to be on the WMP, but is not indicated in PC-III, then he or she would be unrightfully sent on other assignments. This should be an easy catch since the information is readily on the screen, but respondents could simply assume it is there and not look for it. This deception could be considered masking or inventing depending on the objective of the manipulator.

### **Scenario 7**

A SSgt in your squadron wants to re-enlist. Your commander is new to the unit and wishes to know if he (the SSgt) is eligible to reenlist. His name and SSAN is provided below. Is the SSgt eligible for re-enlistment? (Reenlistment/Separation Data)

Butts, Larry A.

123452270

#### Description of Deception

This is a clean scenario without deception. The respondents will look into the reenlistment/separation data to find that SSgt Butts is ineligible to reenlist due to High Year Tenure (HYT). In other words, SSgt Butts has been in the service as long as his rank will allow. Since he did not get promoted to a higher rank in the specified time, he will not be allowed to reenlist.

### **Scenario 8**

Recently, there has been a change in area code for some of the members of your unit. On a recent recall, it was learned that four of the members failed to get their phone numbers changed in the sytem. Pull the phone numbers of those four members and check to ensure the phone numbers are correct. The area code for each should be: 228 Do all of the members now have correct phone numbers? (Circle one) Yes. No. (Individual's Data)

Berry, Michael, S. Jr.	123272801
Bessert, Leona, M.	123379045
Boston, Ambrose, D. Jr.	123424064
Bova, Katherine, M.	123099748

### Description of Deception

Ensuring members have correct telephone numbers is an essential function of Personnel specialists; especially those who work on Commanders' Support Staffs. The telephone number data in PC-III is often used to support the creation of unit recall rosters. Recall rosters provide the means for commanders to quickly assemble their troops in times of emergency. Incorrect telephone numbers mean slower recall and the expenditure of unit resources in order to contact the necessary troops. In this scenario, two of the members have erroneous telephone numbers. In fact, one individual has a "900" number listed. While it is not against regulations to be without a telephone, it is prohibited to have such a number listed as part of a member's records.

This should be fairly easy manipulation for most people to find.

### **Scenario 9**

The first sergeant is doing a dependent care review and has some concerns regarding the four members listed below. He wants to know the number of dependents each of these members have including the number of adult and minor dependents. Please note the number of dependents for each member. (Individual's Data)

Bowling, Kathy A.	123267590
Brinsfield, Michael A.	123238235
Brundidge, Marvin C.	123549902
Carter, Anthony, W.	482460473

Member	Number of Dependents	Adult	Minor
--------	----------------------	-------	-------

### Description of Deception

The dependent care program is designed to ensure dependents are cared for when a military member is called for deployment away from his or her home base. In times of emergency, those military and civilian personnel remaining on the base are often assigned to assist the deployed members dependents. By doing so, the deployed member can carry out his/her assignment with reduced concern for his/her family members at home. The larger the number of dependents left behind, the more difficult the task. In some cases, members will not be deployed (good for promotion to be deployed) if the dependent care burden is too cumbersome. Further, less qualified members may be deployed instead. In this scenario, one of the members listed above has seven

dependents, five of whom are adult dependents. While this is possible, it is not probable and should be considered suspect. This is another form of 'inventing' information. This may be somewhat more difficult for subjects to catch. While they may report their findings for the scenario, they may not flag it as a possible deception.

### **Scenario 10**

A Training Group commander wants to select a Top Tech team. All candidates must have at least one year time on station, must have a Personnel AFSC or Communications AFSC, and must have a "T" prefix. Do all candidates meet the criteria? (Circle one) Yes. No. (Duty Assignment Info, p2)

Carpet, Adam W.	123560733
Cash Naomi	123425067
Chihuahua, Taylor	403449417
Coakley, Howard E.	123280484

### **Description of Deception**

Top Tech is a competition for Air Force instructors. Competing in Top Tech is considered an honor for only the most capable instructors on a training base. Winning the competition is a boon to the instructor and the base. Thus, only the best instructors are selected to attend. Usually the first step is to determine who the qualified instructors are. In this scenario, the respondents must pull the data in the listed individuals and determine if they meet the selection criteria. However, in this scenario one of the members has an AFSC indicating that he is a novice in his field. This individual erroneously has a "T" prefix. A discussion of AFSCs and prefixes can be review in the description of deception section in Scenario 3 above. Since the supporting evidence point to selecting the member with erroneous data, this deception can be consider ????? in the taxonomy. This is a rather difficult deception to detect and it should separate the experience Personnel specialist from the novice.

### **Scenario 11**

A member of your squadron has two Article 15s. Check the disposition dates to determine when the UIF entries will close out. The name and SSAN are provided below. Which entry will close out first? (EPR Info)

Brown, Anthony	123423889
----------------	-----------

### Description of Deception

This is a clean scenario. Airman Brown does indeed have to Article 15s (records of nonjudicial punishment) in his unfavorable information file (UIF). While a commander may close out an Article 15 early, they automatically close out after two years. The respondents merely have to look at the record to determine which closes out first. While this scenario is clean, the many loopholes and variations in the Article 15 system would make it an easy target for strategic information manipulation.

### **Scenario 12**

A Wing Commander wants to ensure consistency in duty titles (i.e. all squadron commanders have duty titles as squadron commanders) For the following members, run and inquiry on their duty titles and supervisors duty title. Are they pretty much consistent? (Circle one) Yes. No.  
(OPR Info)

Halsrud, Clyde E.	123481702
Brundidge, Marvin C.	123549902
Amato, Gerard, A.	123426962
Fisher, William, K.	123575680

### Description of Deception

Duty titles play an important role in the Air Force, much like they do in many civilian businesses. Often members are considered for special duties and new assignments based on their duty titles. Also, a list of duties titles is included in the promotion brief (a summary of an officer's career) for each officer's record at a promotion board. Problems with duty titles can be detrimental to an officer's career. In this scenario, the subjects are asked to look for consistency in the officers' duty titles and their supervisors' duties titles. However, one of the officers has a duty title that is not commensurate with his rank and position in the Air Force. In fact, his duty title indicates he should has a job at a higher echelon than his supervisor. This may be a moderately difficult catch for novices, but fairly easy for seasoned Personnel specialists. This deception might be considered ????? in the taxonomy.

### Scenario 13

TSgt Anderson came to you complaining that none of her dependents seem to have Delta Dental coverage. Use PC-III to see if TSgt Anderson's even has dependents. How many, if any, are noted in the system? \_\_\_\_\_ (Individual's Data)

Anderson, Darlene R.            123315722

#### Description of Deception

TSgt Anderson has 6 dependents noted in the system. While this is not unusual, the birth dates of her dependents and her marital status should arouse some suspicion. All of her dependents have birth dates in the same two years. Also, TSgt Anderson is in the system as single. This record should be highly suspect. An erroneous number of dependents could result in extra pay, additional dependent care duties, deployment concerns, and faulty housing allocations. Respondents could simply answer this question by seeing that dependents were listed in the system without looking at the number. They could also look at the number of dependents, but not the dates. The deceptive practice taking place here is known as *mimicking*.

### Scenario 14

The MPF commander wants to review the last four winners of the Wing NCO of the Quarter award to look for trends. Their names and SSANS are provided below. Run an inquiry on their AFSCs and Duty Titles. Do you see any trends developing (i.e. all with the same AFSC or Duty Title)? (Circle one) Yes. No. (Duty Assignment Data)

Aster, Sylvester, E.	123266839
Angel, Vincent R.	123456474
Ballard, Mary B.	123428256
Bauman, Dan L.	123395521

#### Description of Deception

This deception is slightly more difficult than the others. Sgt Angel is a student. The other NCO's have duty titles commensurate with individuals who might win quarterly awards. It is not possible for a student to win a Wing quarterly award. In order to win, a candidate must demonstrate outstanding duty performance and compete at a formal board. On training bases, only permanent party personnel may compete. Students are

not authorized. A respondent who answers this question can easily answer no due to the inconsistency of Angel's duty title. However, it remain to be seen if the respondent will contemplate the significance of the deviant title. This deceptive tactic might be referred to as *double play*.

### Scenario 15

Four airmen are being considered for a TDY. Their unit commander wants to select the airman with the most time on station for the job. Their names and SSANs are provided below. Which airmen should be the one to go TDY. (Duty Assignment Data, p2)

Achille, Marie M.	123593620
Manchester, Bertha L.	123551911
Bisbee, Thomas G.	123016562
Bratton, Jacob A.	123435231

### Description of Deception

This should be an easy catch for the more experienced personnel. Some of the troops are students. As such, they are not authorized to go on a temporary duty assignment (TDY). Some of the other troops have pending permanent change of station (PCS) assignments. These people are also unauthorized to go on the TDY. Failure to catch these discrepancies could lead to unfulfilled missions, loss of valuable time, and significant confusion for the member selected, the TDY commander, and other with individuals with a stake in the assignment. This deception technique is another form of *mimicking*.

### Scenario 16

A Wing commander has learned that the next 4 personnel who leave the base will not be replaced for 6 months. Candidates A thru D below are possible losses. Pull the duty title, time on station information, and tour status for each. Who will be the first to leave. (Duty Assignment Data, p2)

Charles Haddon Spurgeon	123347385
Anderson, Darlene R.	123315722
Amato, Gerard, A.	123426962
Davis, Claude, A.	123416927

### Description of Deception

In this scenario, all but Amato have information in their records that would disqualify them from an assignment. Likely, many respondents will focus on each members "Date Arrived Station" information to determine who has been on base the longest. A closer look at each record however would reveal that one member is on a controlled tour (must stay on base for 3 years). The other members have derogatory information indicating they cannot leave until it is closed out. This will take some time. When personnel are PCS'd without a replacement, a losing commander has many choices to make. For example, they must decide whether to leave that position unfilled or fill it from the available resources on base (at the cost of another position). Identifying the wrong person in this case can have a chain reaction effect of confusion. The selected member, the person designated to fill the position (if any) and his or her supervisors, the assignments element of the Military Personnel Flight are all affected by this decision. This deceptive practice could be identified as *dazzling*.

### **Scenario 17**

Capt Halsrud is a flight commander of a training squadron. This is important to him because he believes this job will get him a "C" prefix on his AFSC which will show in his record that he has had some command time. Is he in a duty position that will allow him to have an "C" prefix. (Duty Assignment Data, p2)

Halsrud, Clyde E.

123481702

### Description of Deception

This is a clean scenario, but Captain Halsrud is in a position with a "T" prefix even though he has a duty title that might suggest otherwise (e.g., Flight Commander). Thus, Captain Halsrud will not get credit for command time.



## Scenario 18

The first sergeant of your unit heard that a few people living in the dorms were "ghosting." That is, they have assigned dorm rooms, but they choose to spend their own money and live off-base. Often people who ghost change their address so their pay statements and other AF correspondence go to their off base addresses. Check the addresses of these personnel to determine if they still maintain dorm addresses. Do any have off-base addresses? (Circle one) Yes. No. (Individual's Info)

Gretta, James S.	123268867
Griffin, Donald W.	123300604
Boykin, Bobbie, G. Jr.	123559859

### Description of Deception

This is a clean scenario. Often military members are assigned quarters on base and do not use them. This can cause hardships for other military members when base quarters are scarce. Unit First Sergeants have a responsibility to ensure their assigned dormitories are used efficiently. When individual "ghost," they waste needed resources. In this scenario, PC-III indicates two of the three members on the list are ghosting.

## Scenario 19

For NCOs have been selected to attend the NCO Academy in residence. Their names and SSANs are provided below. Your commander believes one of the NCOs is overweight and may be on the weight management program (WMP). Use PC-III to determine if any of these NCO is on the WMP. If any, write the name(s) on the line below. (EPR Info)

---

Lythgoe, Clare J.	123528040
Marbut, Elizabeth, D.	123328687
Mathis, Gary W.	123424048

### Description of Deception

In this scenario, one of the members listed, Marbut, already attended the Academy. The goal here is to decoy respondents from noticing this situation. This scenario has respondents examining WMP information. The professional military education information like NCO Academy attendance is also noted. If a respondent only looks at WMP information, Marbut would be recommended for attendance. Resources would be

expended to send her only to find out later that she also ready attended. While this appears to be a small consequence of the deception, it wastes Tsgt Marbut's time, her supervisor's time, the resources of the Personnel flight, and more. This deception is best described as *decoying*.

## Scenario 20

A new squadron commander (Lt Col Whitley - 123221342), wanted to know whose performance reports (EPRs, OPRs,) he rated. List the names, grades, and duty titles of the personnel he rates in the blank area to the right of the steps to produce the report listed below.

To answer this question: (Note + = transmit)

1. Go to reports and rips in the opening menu+
2. Select reports+
3. Select Performance Reports+
4. Combined...+
5. Rater's Subordinate...+
6. Enter Supervisor's SSAN+
7. F3 (Back to main menu)
8. Office Automation...+
9. Products+
10. Select Report+
11. View and Pg Dn

### Description of Deception

This scenario increases the task complexity of the assignment. Personnel specialists are often required to use PC-III to produce reports. Rather than just make in query into the system, this scenario requires the respondents to produce a "Rater's Subordinate" report. In this manner, respondents can identify Lt Col Whitley's subordinates as they are maintained in the system. However, in this scenario, one of the subordinates has a title of "Wing Commander." This cannot be right for two reasons. First, a Wing Commander is never subordinate to a Squadron Commander. Second, a Lt Col can only be the superior of those of a lesser rank. Wing Commanders as typically full Colonels or one-star generals. This deceptive information, if unchecked, could disrupt the assignment process, performance reports, awards and decorations, and a host of other areas. While it is not life-threatening or detrimental to a mission, its repair will consume valueable resources. The longer it goes unchecked, the more transactions it will influence. In turn, more and more resource will have to be devoted to cleaning it out of the system. This tactic might be considered *repackaging*.

**APPENDIX C**  
**PC-III SCREENS**

### PC-III Screens

This appendix provides illustrates of the PC-III Screens the respondents must examine in order to collect the information they need to answer the scenarios. The font used is similar to the font on the actual PC-III screen.

#### Enlisted Data Qualification, Page 1

Qualification Data - Amn				Page
1 of 2				
Grade: AMN		Name: GRAY CHRISTIAN A		SSAN: 123565450
CAFSC:	2E211	CAFSC Eff Date:	9504	CAFSC SEI:
PAFSC:	2E211	PAFSC SEI's:	/ / / /	
2AFSC:		2AFSC SEI's:	/ / / /	DAFSC:
2E211				
3AFSC:		3AFSC SEI's:	/ / /	DIERT:
000000				
4AFSC:		4AFSC SEI's:	/ /	
General SEI:		Training Status Id/Text/Date: K/TECH SCH 3LVL AWD		
/930907				
Amn Aptitude Test Id: Admin - 74 Elect - 73 Gen - 68 Mech - 85				
Professional Military Courses		Date Completed	Method of Study	
1.				
2.				
3.				
Education Level		Date	Speciality	
Method				
1.	HSDP HS DIPL	9306	N/A	N/A
2.	NONE		N/A	N/A
3.	NONE		N/A	N/A
INSTRUCTION: 1. Press the "Space Bar" to go to the next page ->				

**Enlisted Qualification Data, Page 2**

Qualification Data - Amn

Page 2 of 2

Lang Id 1st: N/A

Read Code/Text: /NEVER TESTED

Listen Code/Text: /NEVER TESTED

Speak Code/Text: /NEVER TESTED

Lang Id 2nd: N/A

Read Code/Text: /NEVER TESTED

Listen Code/Text: /NEVER TESTED

Speak Code/Text: /NEVER TESTED

Pers Scty Clear Status: SECRET

Scty Inv Type: ENTNAC

Date Scty Inv Comp: 920902

Scty Clear Stat Date: 920902

PRP Status: N/A

PRP Status Date:

Press transmit key to continue or "Space Bar" to return to 1st page->

## Airman Service Dates

Service Dates - Amn

Grade: A1C Name: BALAKIT MACARIO B JR

SSAN: 123035446

Pay Date: 930601	DOS: 970531	Svs Component: REGULAR
Ead Date: 930601	ETS: 970531	Cat of Enlistment: 1
TAFMSD: 930601	TEMSD:	Term of Enlistment: 4
Lost Days:	UIF-ID:	Mil Svs Obligation: 8
DEROS:		

ADSC/RSN 1st: / NOT APPLICABLE

Duty Status: 00	Projected Duty Status:
Eff Date: 000000	Eff Date:
Exp Date: 000000	Exp Date:
Reenl Elig:NO AFSC AWARDED WHICH IS COMMENSURATE WITH GRADE	

### INSTRUCTIONS:

1. Press the "F2" key if you want an explanation of the data above; or
2. Press the "ESC" key to quit. ->

## Awards and Decorations, Page 1

Awards and Decorations		Page 1 of 2	
Grade: A1C	Name: BALAKIT MACARIO B JR	SSAN: 123035446	
Military Decorations	Number	Date	Non Military Dec
MERIT SVC MEDAL	03	980202	
			Foreign
Decorations			
Unit Citations	Devices	Foreign Awards	Devices
N/A		N/A	
N/A		N/A	
N/A		N/A	
N/A		N/A	
N/A		N/A	
N/A			
Number AF Good Conduct Medals-Date Last AFGCM-AFGCM Start Credit Svc			
Date NO AWARD			
Press "Space Bar" to go to the next page ->			

## Awards and Decorations, Page 2

Campaign Service Awards

Page 2 of 2

Grade: A1C      Name: BALAKIT MACARIO B JR      SSAN: 123035446

Campaign Service Awards      Devices

1. AF TRAINING RBN	11. N/A
2. N/A	12. N/A
3. N/A	13. N/A
4. N/A	14. N/A
5. N/A	15. N/A
6. N/A	16. N/A
7. N/A	17. N/A
8. N/A	18. N/A
9. N/A	19. N/A
10. N/A	20. N/A

Press transmit key to continue or "Space Bar" to return to 1st page->



## EPR Information, Page 1

### EPR Information

Grade: A1C Name: BALAKIT MACARIO B JR SSAN: 123035446

Last Evaluation:	Date Supervision Begins:
Close-Out Date Last EPR:	Supervisor's SSAN:
Reason For Next EPR: N/A	Proj Date Suprvn Begins:
Date Next EPR Proj:	Office Symbol: CCQ
Duty Title: STUDENT	
DAFSC: 3C211	Duty Phone: 6013773803

### Grade Information

Current Grade: A1C	Projected Grade:
Current Grade Date of Rank: 930601	Projected Grade Date of Rank:
Current Grade Effective Date: 930601	Projected Sequence Number:
Promotion Eligibility Status Airman: X	
Promotion Eligibility Status Effective Date: 9306	
Promotion Eligibility Status Expiration Date:	

SPACEBAR to go to page 2.....

Page 1 of 3

## EPR Information, Page 2

### QUALITY CONTROL FACTORS

Unfavorable Information/Control Roster ID: NO -NO UIF AND NOT ON CNTL ROSTER

Unfavorable Information File (UIF) Disposition Date:  
Substance Abuse Control Source: N/A  
Substance Abuse Trans Type: N/A  
Weight Management Program Initial Entry Date:  
Weight Status Code: N/A  
Weight Status Date:

### EDUCATION INFORMATION

-----  
Education Level:            Date    Specialty:            Method:

1) <4YR >90 SH OR >135 QH 8803    INTER-AREA SPECIALIZATIONS

2) NONE	N/A	N/A
3) NONE	N/A	N/A

SPACEBAR to go to page 3.....

Page 2 of 3

### EPR Information, Page 3

#### PROFESSIONAL MILITARY EDUCATION INFORMATION

Course Completed:      Date Completed:      Method of Study:

1.   None

#### DECORATION INFORMATION

Military Decorations:	Number:	Date:
MERIT SVC MEDAL	03	980202

SPACEBAR to go to page 1 OR TRANSMIT to continue.....  
Page 3 of 3

## Duty Assignment Data, Page 1

### DUTY ASSIGNMENT DATA

Page 1 of 2

Grade: A1C Name: BALAKIT MACARIO B JR

SSAN: 123035446

Deployment Availability Status

EXP Date:

Admin:

Phys:

Legal:

Time: PROJECTED SEPARATION WITHIN 180 DYS

970531

PRP Status:

PRP Status Date:

Duty Status: 00

Projected Duty Status Date:

Duty Status Eff Date: 000000

Projected Duty Status Eff Date:

Duty Status Exp Date: 000000

Projected Duty Status Exp Date:

Current Avn Svc Cd: -NOT APPLICABLE

### INSTRUCTIONS:

Press the "Space Bar" to go to the next page -> ; or the "ESC" key to quit.

## Duty Assignment Data, Page 2

DUTY ASSIGNMENT DATA

Page 2 of 2

Date Arrive Station: 930715  
Date Departed Last Duty Station: 930715  
Duty Effective Date: 930715      Duty Position Number: 0000000  
Duty AFSC: 3C211      Duty Command Level: STUDENT  
Duty Title: STUDENT  
Organization Structure ID:  
Functional Account: 499900  
Duty Location: MAHG  
Functional Category: BMTS/OFF ACCESS  
Program Element: 84731C

Assignment Limitations:

Exp Date:

1. N/A
2. N/A
3. N/A

Assignment Availabilities:

Exp Date:

1. NO DEFERMENT
2. NO DEFERMENT
3. NO DEFERMENT
4. NO DEFERMENT

Press the transmit key to quit, or "Space Bar" to return to 1st page ->

## Individual's Data

### INDIVIDUAL DATA

Grade: A1C Name: BALAKIT MACARIO B JR SSAN: 123035446  
Office: CCQ Duty Phone: 6013773803 Home Phone:

PAS Code: 335 TRS  
Mailing Address  
PSC Box 4217

Residence Address  
Bldg 148, Rm 119

Place of Birth: CA

Date of Birth: 650624

Sex: M Race: OTH

Ethnic Group: FILIPINO

Religion: ROMAN CATHOLIC CHURCH

Citizenship Status: BY BIRTH IN UNITED STATES

Marital Status: M Total Dependents: 01 Adults in Household:

Children in Household: , , , , , ,

Mil Stat Spouse: N/A

Jt Asg Intent: N/A

Spouse's SSAN:

INSTRUCTIONS: (For explanation of terms, press the "F2" key.)

1. Press transmit key to quit.->

## Reenlistment/Separation Data

### REENLISTMENT/SEPARATIONS INFORMATION

Grade: SSG      Name: BUTTS LARRY A      SSAN: 123452270  
Record Type: AA  
DOS: 980818      ETS: 940818      HYT Date: 9906

Existing Extensions:      ,      ,

Reenlistment/Retirement/Separation Effective Date:  
Application Retirement/Separation DOS Requested:

Reenlistment AFSC:  
Reenlistment Date Requested:  
Reenlistment Bonus Requested:  
Reenlistment Term Projected:

Reenlistment Eligibility Status: 2T  
INELIGIBLE DUE TO HYT AND < 13 MONTHS REMAINING UNTIL DOS  
INSTRUCTIONS:

1. Press transmit key to quit. ->

## OPR Information, Page 1

OPR INFORMATION		Page 1 of 3
Grade: CPT	Name: HALSRUD CLYDE E	SSAN: 123481702
Close Out Date Last OPR: 930204		
Date Supervision Begins: 930520		
Reason For Next OPR: ANNUAL		
Supervisor's SSAN: 033481739		
Date Next OPR Proj: 940204		
Proj Date Suprvn Begins:		
Proj Supervisor's SSAN:		Office Symbol: TTMQEO
Duty Title: COMMANDER, IM COURSES		
Duty Phone: 5790		
DAFSC: T033S3		
GRADE INFORMATION		
Current Grade: 03	Proj Grade:	
Current Grade Date of Rank: 880203		
Proj Grade Date of Rank:		
Current Grade Effective Date: 880203		
Press "SPACE BAR" to go to the next page -> ; or press "ESC" to quit.		



## OPR Information, Page 2

### QUALITY CONTROL FACTORS

Page 2 of 3

Unfavorable Information/Control Roster Id: NO -NO UIF AND NOT ON CNTL ROSTER

Unfavorable Information File (UIF) Disposition Date:

Substance Abuse Control Source: N/A

Substance Abuse Trans Type: N/A

Weight Management Program Initial Entry Date:

Weight Status Code: N/A

Weight Status Date:

### EDUCATION INFORMATION

Ed Level Highest: BAC AWD BACHELORS DEGREE

Year Completed: 77

Specialty: EDUC, SEC TEACH, MUSIC

Method: NONE/NOT APPL

Ed Level 2nd Highest: NONE

Year Completed:

Specialty: N/A

Method: N/A

Press "SPACE BAR" to go to next screen or press "ESC" to quit .... ->

### OPR Information, Page 3

#### PROFESSIONAL MILITARY EDUCATION INFORMATION

Page 3 of 3

Course Completed:	Date Completed:	Method of Study:
SQ OFF SCH	87	RES + COR

#### DECORATION INFORMATION

Military Decorations:	Number:	Date:
AF COMM MEDAL	03	920407
AF ACHVMT MDL	01	840831

Press the "SPACE BAR" to return to 1st page or "TRANSMIT" key to quit.....

**APPENDIX D**  
**DISCREPANCY REPORTING SHEET**

## Discrepancy Reporting Sheet

Use this Discrepancy Reporting Sheet to note any possible discrepancies you may find. To aid in our efficient correction of possible problems, please note, the approximate time in the exercise you noticed the discrepancy, the scenario number, and the nature of the discrepancy. Your help in enabling us to improve our curriculum will benefit students for many classes to come.

Time	Scenario #	Nature of the Discrepancy
:05		
:10		
:15		
:20		
:25		
:30		
:35		
:40		
:45		
:50		
:55		
:60		
1:05		
1:10		
1:15		
1:20		
1:25		
1:30		

**APPENDIX E**

**STRATEGY OF MANIPULATIONS**

## **Strategy of Manipulations**

Probably one of the more important decisions to make in this research endeavor was the determination of what type of manipulations to include. The level of difficulty of the manipulations must also be considered. This appendix outlines the strategy used in building the experiment and discusses the factors considered in manipulation development.

The main focus of the manipulation strategy was to adequately represent the tactics outlined in the taxonomy (Johnson, et al., 1993). While not every deceptive tactic could be included, the majority was well represented. The previous appendix highlights how the tactics were used for each scenario. The authors of the taxonomy point out that not every tactic can be used in every information system (Ibid.).

Besides the focus on the taxonomy, other factors influenced the manipulation strategy as well. While the amount of deceptive information is discussed in Chapter 4, the level of deception must also be considered. Level of deception refers to the difficulty of identify a manipulation piece of information as a deception. Considering that many of the respondents are novices to the information domain and had only formal training on PC-III or simulators, some of the deceptions had to be easily detectable. This was also necessary for to test the appropriateness of Information Manipulation Theory (McCornack, 1990). For instance, Scenario #2 involves an Airman First Class (A1C) with three Meritorious Service Medals (MSMs). This should be relatively easy for even novices to catch. Most airmen learn about rank structure and awards and decoration in

their basic training. The novice respondents involved in this experiment not only had that training, but their Personnel curriculum also covers these topics. Thus, they did have the knowledge to identify this discrepancy.

Other scenarios had more difficult deceptions to detect. For example, on scenario involved a student with a "T" prefix on is Air Force Specialty Code. Such a prefix is an indication that the individual is in an instructor's duty position. A student cannot fill that position. In order to catch this deception, a respondent must be experienced enough to understand what a "T" prefix means. The objective here was not to ensure there were scenarios that novice would miss. Rather, the goal was to provide for a well-rounded representation of possible manipulations.

Another factor involved in the manipulation strategy was the relevance to the real world situations the respondents would typically face. Every scenario included in the experiment will likely be encountered by all of the respondents at some point in their careers. Some of the scenarios appear as if a commander should be answering the question. However, it is the Personnel specialists who act as information retrieval specialists for commanders. They are often relied upon to retrieve the information and highlight the likely answer for the commanders. Often the commanders are not as well acquainted with the information domain as the Personnel specialists. As such, commanders must often rely on the judgement of their subordinates.

The final factor involved in the manipulation strategy was the leeway offered by PC-III to make the manipulations. PC-III contains a number of system edits and

redundancy checks to help ensure data integrity. The Air Force has been using PC-III for the last 10 years. During that time, more and more edits and checks have been implemented via system upgrades. Thus, the number of actual manipulations that could be made without significant reprogramming is limited. Reprogramming is considered unrealistic for three reasons. First, a perpetrator would have to reprogram both PC-III and a Sperry back-up system. This would not only require significant programming knowledge of the PC-III software, but also considerable knowledge of the information domain. Second, reprogramming PC-III would require a perpetrator to gain access to the necessary files. There are considerable firewalls and other safeguards that would make this easier said than done. Finally, there is no reason to go to all that effort when sufficient manipulations can be made within the constraints of the PC-III system (as demonstrated in the experiment). A perpetrator merely needs user access and a little knowledge of the information domain to cause damage.

In summary, the strategy of for the information manipulations used in the experiment was to provide a good representation of the deception taxonomy and test related theory. Providing for a continuum of detection difficulty levels was necessary to test the influence of experience in the domain on deception detection ability. Finally, designing scenarios and manipulations to represent real world tasks and fit within the constraints of the PC-III system added realism to the experiment.



**APPENDIX F**

**DECEPTION TAXONOMY LESSON PLAN**

## **Deception Taxonomy Lesson Plan**

The following lesson plan was developed in accordance with the Air Force's Air Education and Training Command's (AETC) guidelines for lesson plan development. All curricula taught in AETC must follow these guidelines and correspond to an appropriate item on a Course Training Standard (CTS). The CTS is document by which courses instructors and training developers get their course curriculum mandate by functional representatives in each of the major commands.

The lesson plan was created in that manner for a number of reasons. First, the researcher wanted to provided students with as much realism as possible. Not only did the lesson plan fit the AETC criteria, but the researcher wore his instructor's badge and followed ATEC norms while conducting the training. Second, it is possible that some of the respondents were former instructors. If so, they would become suspicious if an instructor was not following AETC guidelines. Finally, Personnel instructors indicated a desire to include more computer security training in their courses. Along with the scenarios, they were provided with an electronic copy of the lesson plan.

<b>Lesson Plan Part II - Teaching Guide</b>		
<b>Body (1/2 Hour)</b>		
<b>Presentation</b>	<b>L, DS</b>	<b>1/2 Hour</b>
2a. Identify fact Pertaining to Deception Detection in Information Systems (STS: Reference) Meas: W	OVERVIEW:	
(1) Reference	KPA 18-3-1	
(2) Purpose		
(a) Increase awareness of methods hackers may use to influence decision making by Air Force personnel by corrupting data in Air Force computers.	<p><b>People often belief that hackers want to simply destroy data and bring computers down.</b></p> <p><b>Some hackers want to change data in Air Force computers in an attempt to get Air Force members to make bad decisions.</b></p>	
(3) Tactics for Deception		
(a) Masking	<p><b>This tactic consists of deleting information that may suggest the correct decisions.</b></p> <p><b>Ex. Deleting the skill level of an experienced personnel NCO from a possible deployment listing.</b></p>	
(b) Double Play	<p><b>This tactic is used to weakly suggest a correct decision. The idea is to only weakly support the correct answer which may reinforce the correct decision. Usually the incorrect answer also has strong reinforcement.</b></p>	
(c) Mimicking	<p><b>Modify the information to suggest an incorrect decision.</b></p> <p><b>Ex. Adding an erroneous header to a computer printout (RIP)</b></p>	

(d) Dazzling	<p><b>Adding information to blur the correct answer and emphasize the incorrect answer.</b></p> <p><b>Ex. Rather than marking someone down on an EPR, noting the their problems in the narrative.</b></p>
(e) Inventing	<p><b>Just as the name implies, inventing is the tactic of adding information to support an incorrect decision.</b></p> <p><b>Ex. Adding a degree to a person's education records in an attempt to get him or her selected for an assignment.</b></p>
(f) Repackaging	<p><b>Modifying attributes in the environment to hinder the generation of the correct representation.</b></p> <p><b>Ex. Adding notes to a PC-III printout that may misrepresent a UIF status.</b></p>
(g) Decoying	<p><b>Adding an attribute that directs attention away from the correct attribute.</b></p> <p><b>Ex. Changing a duty title to make a decision maker think an unqualified troop is an appropriate candidate for a special assignment.</b></p>
(4) Detecting the Deception	
(a) Awareness	<p><b>Simply being aware that these deceptive tactics exist is part of the battle.</b></p>
(b) Hypothesizing	<p><b>Another method is to create and test a quick hypothesis about the deception.</b></p> <p><b>Ex. You might suspect some information about a member's EPRs. Test the hypothesis by calling the member's squadron to confirm the information.</b></p>
	TRANSITION

**APPENDIX G**  
**SURVEY INSTRUMENT**

## Attitude Toward PC-III Usage Scale

### INSTRUCTIONS

This is a short two-part survey to determine your experience level in Personnel and your trust in PC-III. Please respond to the following items to the best of your knowledge or ability. Respond to the items in Section I by filling in the blanks as required. Respond to the items in Section II by filling in the circle that best represents your feelings toward each statement regarding PC-III.

### SECTION I - Personnel Career Experience (Please fill in the blanks)

1. Are you in the Airman, Officer, or Craftsmen course. (Circle one)
2. Amount of time you've been in the Personnel career field: \_\_\_\_\_.

**Note: If this course is your first experience in the Personnel career field or you answered 3 months or less in question #2, please skip to Section II**

3. What echelons within the personnel career field have you worked?  
(e.g. HQ USAF, AFPC, MAJCOM, FOA, DRU, MPF, CSS, or GSU) (Please circle all that are applicable.)

PLEASE ANSWER THE FOLLOWING QUESTIONS IN MONTHS!!

4. How much experience do you have working on a Squadron Commander's Support Staff? \_\_\_\_\_
5. How much experience do you have in Customer Support (include offices such as Customer Service, Casualty, Personal Affairs and Records)? \_\_\_\_\_
6. How much experience do you have in Career Enhancement (include offices such as EPRs/OPRs, Reenlistments, Promotions, and Awards/Decorations)? \_\_\_\_\_
7. How much experience do you have in Personnel Relocations and Employment (include offices such as Separations, Retirements, and Assignments)? \_\_\_\_\_
8. How much experience do you have in INTRO (Individualized Newcomer Treatment and Orientation)? \_\_\_\_\_

9. How much experience do you have in the Manning Control Unit? \_\_\_\_\_,  
Formal Training? \_\_\_\_\_, and Retraining? \_\_\_\_\_

10. How much experience do you have in the Personal Readiness Unit? \_\_\_\_\_

## SECTION II - PC-III Trust Scale

## SECTION II - PC-III Trust Scale

Please indicate how you feel about each of the following statements by circling the number corresponding to the following scale.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

1. I know how PC-III is going to perform. ① ② ③ ④ ⑤
2. PC-III performs as I expect it to. ① ② ③ ④ ⑤
3. I have found that PC-III is thoroughly dependable. ① ② ③ ④ ⑤
4. PC-III tends to behave quite variable (erratic). ① ② ③ ④ ⑤
5. Based on past experience, I cannot with complete confidence rely on PC-III to provide reliable information. ① ② ③ ④ ⑤
6. PC-III is a very sound system and even if PC-III were to provide questionable information, people should feel confident that they are getting the information they need to do their jobs. ① ② ③ ④ ⑤
7. PC-III is not very predictable. People can't always be certain how PC-III will perform from one day to another. ① ② ③ ④ ⑤
8. I am very familiar with the operational behaviors of PC-III and it will perform in certain ways. ① ② ③ ④ ⑤
9. Even in familiar circumstances, I am not totally certain PC-III will act the same way twice. ① ② ③ ④ ⑤

10. I feel completely secure in performing new information-related tasks because I can depend on PC-III to provide the information I need. ① ② ③ ④ ⑤
11. PC-III is not necessarily a system others consider reliable. ① ② ③ ④ ⑤
12. I can think of some times PC-III could not be counted on. ① ② ③ ④ ⑤
13. PC-III has not always been trustworthy in the past, and there are times when I am hesitant to rely on PC-III to provide accurate information for me to do my job. ① ② ③ ④ ⑤
14. PC-III behaves in a consistent manner. ① ② ③ ④ ⑤



**APPENDIX H**  
**ADDITIONAL SCALES**

## Attitude Toward Computer Usage

### INSTRUCTIONS

This is a short two-part survey to determine your attitude toward computers and PC-III. Please respond to the following items to the best of your knowledge or ability. Respond to the items in Section I by circling the response that best represents your individual use of, beliefs, knowledge about, and interactions with computers and computer-related mechanisms. Respond to the items in Section II by placing a check on the each line that you see to show what you think about the quality of the data in PC-III.

### DEMOGRAPHICS (Please fill in the blank)

1. Level of highest education (e.g. high school, Bachelor's degree): \_\_\_\_\_.
2. Number of formal computer course you've taken: \_\_\_\_\_.
3. Amount of time you've been in the Personnel career field: \_\_\_\_\_.
4. How long have you worked with PC-III? \_\_\_\_\_.
5. Approximate percentage of duty day spent on PC-III: \_\_\_\_\_.

### SECTION I - General Computer Usage

Please indicate how you feel about each of the following statements by circling the number corresponding to the following scale.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

1. I would prefer to type a paper on a word processor than on a typewriter. ① ② ③ ④ ⑤
2. Whenever I use something that is computerized, I am afraid I will break it. ① ② ③ ④ ⑤
3. I like to keep up with new technological advances. ① ② ③ ④ ⑤

4. I know that I will not understand how to use computers. ① ② ③ ④ ⑤
5. Using a computer is too time consuming. ① ② ③ ④ ⑤
6. I feel that having a computer at work would help me with my job. ① ② ③ ④ ⑤
7. I prefer not to learn how to use a computer. ① ② ③ ④ ⑤
8. I would like to own, or I do own a computer. ① ② ③ ④ ⑤
9. I like to play video games. ① ② ③ ④ ⑤
10. I feel that the use of computers in schools will help children learn mathematics. ① ② ③ ④ ⑤
11. I prefer to use an automatic teller (ATM) for most of my banking. ① ② ③ ④ ⑤
12. If I had children, I would not buy them computerized toys. ① ② ③ ④ ⑤
13. I have had bad experiences with computers. ① ② ③ ④ ⑤
14. I would prefer to order items in a store through a computer than wait for a clerk. ① ② ③ ④ ⑤
15. I feel that the use of computers in schools will negatively affect childrens' reading and writing abilities. ① ② ③ ④ ⑤
16. I do not like using computers because I cannot see how the work is being done. ① ② ③ ④ ⑤
17. I would prefer to go to a store that uses computerized scanners than go where the clerks enter each price into the cash register. ① ② ③ ④ ⑤
18. I do not feel I have control over what I do when I use a computer. ① ② ③ ④ ⑤
19. I think that computers and other technological advances have helped to improve our lives. ① ② ③ ④ ⑤

20. I do not like to program computerized items such as VCR's ① ② ③ ④ ⑤  
and microwave ovens.

## SECTION II - PC-III Data Quality

The purpose of this portion of the survey is for you to assess the data quality of PC-III. Please indicate what *you* think of the quality of the data in PC-III. Do not concern yourself with the mechanical operation of the system (e.g. data input, editing), focus solely on data quality.

Please place an X directly on each line. Do not attempt to place an X over two or more lines. Note: If you place an X in the middle space, you consider PC-III data quality to be neutral regarding these two adjectives..

### PC-III Data Quality

Good	_____ . _____ . _____ . _____ . _____ . _____ . _____	Bad
Worthless	_____ . _____ . _____ . _____ . _____ . _____ . _____	Valuable
Clear	_____ . _____ . _____ . _____ . _____ . _____ . _____	Hazy
Correct	_____ . _____ . _____ . _____ . _____ . _____ . _____	Incorrect
True	_____ . _____ . _____ . _____ . _____ . _____ . _____	False
Reliable	_____ . _____ . _____ . _____ . _____ . _____ . _____	Unreliable
Accurate	_____ . _____ . _____ . _____ . _____ . _____ . _____	Wrong

THANK YOU FOR YOUR RESPONSES!

## REFERENCES

- Adams, J.A. (1987). "Criticisms of Vigilance Research: A Discussion," *Human Factors*, 29(6), 737-740.
- Alexander, M. (1990). "Hacker Attacks Can Be Hazardous to Health," *Computerworld*, 24(29), 31.
- Anthes, G.H. (1994). "Experts Probe Threats, Defenses to Net Security," *Computerworld*, 29(1), 81-82.
- Anthes, G.H. (1996a). "Net Attacks Up, Defenses Down," *Computerworld*, 30(3), 71-73.
- Anthes, G.H. (1996b). "US Easy Target for Cyberattacks," *Computerworld*, 30(22), 7.
- Blocher, E.; Moffie, R.P. and Zmud, R.W. (1986). "Report Format and Task Complexity: Interaction in Risk Judgements," *Accounting, Organizations and Society*, 11(6), 457-470.
- Bodnar, G.H. (1993). "Data Security and Contingency Planning," *Internal Auditing*, 8(3), 74-81.
- Boockholdt, J.L. (1989). "Implementing Security and Integrity in Micro-Mainframe Networks," *MIS Quarterly*, 13, 135-144.
- Bowyer, J.B. (1982). *Cheating*. NY: St. Martin Press.
- Brown, T.S.; Brown, J.T., and Baack, S.A. (1988). "A Reexamination of the Attitude Toward Computer Usage Scale," *Educational and Psychological Measurement*, 48, 835-842.
- Buller, D.B. (1988). "Deception by Strangers, Friends, and Intimates: Attributional Biases Due to Relationship Development," Paper presented at the annual meeting of the Speech Communication Association (November), Boston, MA.

- Buller, D.B. and Burgoon, J.K. (1996a). "Interpersonal Deception Theory," *Communication Theory*.
- Buller, D.B. and Burgoon, J.K. (1996b). "Another Look at Information Management: A Rejoinder to McCornack, Levine, Morrison, and Lapinski," *Communication Monographs*. 63(1) 92-103.
- Burgoon, J.K. and Buller, D.B. (1994). "Interpersonal Deception: Effects of Deceit on Perceived Communication and Nonverbal Behaviors Dynamics," *Journal of Nonverbal Behavior*, 18(2), 155-184.
- Burgoon, J.K., Buller, D.B., Eresu, A.S., and Rockwell, P. (1994). "Interpersonal Deception: Accuracy in Deception Detection," *Communication Monographs*, 51, 303-325.
- Burgoon, J.K., Buller, D.B., and Guerrero, L.K. (1995). "Interpersonal Deception: Effects of Social Skills and Nonverbal Communication on Deception Success and Detection Accuracy," *Journal of Language and Social Psychology*, 14(3), 289-311.
- Burgoon, J.K., Buller, D.B., and Guerrero, L.K., Afifi, W.A., and Feldman, C.A. (1996). "Interpersonal Deception: Information Management Dimensions Underlying Deceptive and Truthful Messages," *Communication Monographs*, 63, 50-69.
- Campbell, J.P. (1990). "Modeling the Performance Prediction Problem in Industrial and Organizational Psychology," in Handbook of Industrial and Organizational Psychology (2nd ed.), Dunnette, M.D. and Hough, L. M. (eds.), Palo Alto, CA: Consulting Psychologists Press, 687-732.
- Cobb, S. (1995). "Internet Firewalls," *Byte*, 20(10), 179-181.
- Cook, T.D. and Campbell, D. T. (1979). *Quasi-Experimentation*. Boston: Houghton Mifflin Co.
- Daft, R. L. and Lengel, R.H. (1986). "Organizational Information Requirements, Media Richness, and Structural Design," *Management Science*. 32(5), 554-571.
- Davies, D.R. and Tune, G.S. (1969). *Human Vigilance Performance*. NY: American Elsevier Publishing Company, Inc.

- Davies, D.R. and Parasuraman, R. (1981). *The Psychology of Vigilance*. London: Academic Press.
- Day, K. (1995). "Agencies Quick to Pick Up E-mail, Poll Finds," *The Washington Post*, 118, F1.
- DePaulo, B.M., Stone, J. and Lassiter, G.G., (1985) "Deceiving and Detecting Deceit,"
- DePaulo, P.J. and DePaulo, B.M. (1989) "Can Deception by Salespersons and Customers Be Detected Through Nonverbal Behavioral Cues?," *Journal of Applied Psychology*, 19(18), 1552-1577.
- DeSanctis, G. and Poole, M.S. (1994). "Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory," *Organization Science*, 5(2) 121-147.
- Feeley, T. H. and De Turck, M.A., (1995). "Global Cue Usage in Behavioral Lie Detection," *Communication Quarterly*, 43(4), 420-430.
- Fowler, B.W. and Peterson, D.R. (1997). "Information Age Warfare," *ORMS Today*, 24(2), 34-37.
- Grice, P. (1989). *Studies in the Way of Words*. Cambridge MA: Harvard University Press.
- Grier, P. (1997). "At War with Sweepers, Sniffers, Trapdoors, and Worms," *Air Force Magazine*, 80(3), 20-24.
- Glaser, R. and Chi, M.T.H. (1988)., Overview in Chi, M.T.H. ; Glaser, R.; and Farr, M.J. (eds.), *The Nature of Expertise*. Hillsdale, NJ: Lawrence Erlbaum Associates.
- Goodman, S.E. (1996). "War, Information, Technologies, and International Asymmetries," *Communications of the ACM*, 39(12), 11-15
- Hamilton, D. (1989). "The Bigger They Get the More the Messages Multiply," *Computerworld*, 18(16), 147.
- Huber, G.P. (1983). "Cognitive Style as a Basis for MIS and DSS Designs: Much Ado About Nothing," *Management Science*, 29(5), 567-579.

- Huh, Y.U.; Keller, F.R., Redmond, T.C. and Watkins, A.R. (1990). "Data Quality," *Information and Software Technology* 32(8), 559-565.
- Information Warfare*. (1996) A training publication developed by the United States Air Force Doctrine Division, USAF/XOXD.
- Jacobs, S; Dawson, E.J.; and Brashers, D. (1996). "Information Manipulation Theory: A Replication and Assessment," *Communication Monographs*, 63(1), 70-82.
- Jackson, T. (1995). "Do I Need E-mail?," *The Financial Times*, n32747, 10.
- Janson, M.A. (1988). "Data Quality: The Achilles Heel of End-User Computing" *OMEGA International Journal of Management Science*, 16(5), 491-502.
- Johnson, P.E; Grazioli, S.; and Jamal, K. (1993). "Fraud Detection: Intentionality and Deception in Cognition," *Accounting, Organizations, and Society*, 18(5), 467-488.
- Johnson-George, C. and Swap, W.C. (1982). "Measurement of Specific Interpersonal Trust: Construction and Validation of a Scale to Assess Trust in a Specific Other," *Journal of Personality and Social Psychology*, 43(6), 1306-1317.
- Kornel, Amiel. (1989). "LAN E-mail to Skyrocket, Survey Finds," *Computerworld*, 23(37), 60-61.
- Klein, B.D. (1996) "Error Detection and Correction in Actural Data" in M. Khosrowpour (Ed.) *Proceedings of the 1996 Information Resources Management Association International Conference*, 73-79. Washington D.C., Idea Group Publishing.
- Klein, B.D.; Goodhue, D.L., and Davis, G.B., (1997a). "Can Humans Detect Error in Data? Inpact of Base Rates, Incentives, and Goals," *MIS Quarterly*, 21(2) 169-194.
- Klein, B.D.; Goodhue, D.L., and Davis, G.B., (1997b). "Conditions for the Detection of Data Errors in Organizational Settings: Preliminary Results from a Field Study." Unpublished manuscript.
- Knight, B. (1992). "The Data Polution Problem." *Computerworld*, 26(39), 81-83.
- Koslowsky, M.; Lazar, A. and Hoffman, M. (1988). "Validating and Attitude Toward Computer Scale," *Educational and Psychological Measurement*, 48, 517-521.



- Larkin, J.; McDermott, J.; Simon, D.P.; and Simon, H.A. (1980). "Expert and Novice Performance in Solving Physics Problems," *Science*, 1335-1342.
- Laudon, K.C. (1986). "Data Quality and Due Process in Large Interorganizational Systems," *Communications of the ACM*, 29(1), 4-11.
- Levine, T.R. and McCornack, S.A. (1991). "The Dark Side of Trust: Conceptualizing and Measuring Types of Communicative Suspicion," *Communication Quarterly*, 39(4) 325-340.
- Levine, T.R. and McCornack, S.A. (1992). "Linking Love and Lies: A Formal Test of the McCornack and Parks Model of Deception Detection," *Journal of Social and Personal Relationships*, 9, 143-154.
- Libicki, M.C. , (1995). "What is Information Warfare?" National Defense University Strategic Forum, 28, 1-4.
- Mackworth, N. H. (1950). *Researches on the Measurement of Human Performance* (Medical Council Special Report Series 268). London: His Majesty's Stationery Office.
- Maier, N.R.F. and Thurber, J.A. (1968) "Accuracy of Judgements of Deception When an Interview is Watched, Heard, and Read," *Personnel Psychology*, 21, 23-30.
- Malik, W. (1996) "Information Warfare," *GartnerGroup Research Note*, KA-SMG-103.
- McCornack, S.A and Levine, T.R. (1990), "When Lovers Become Leery: The Relationship Between Suspicion and Accuracy in Detecting Deception," *Communication Monographs*, 57, 219-230.
- McCornack, S.A. and Parks, M.R. (1986), "Deception Detection and Relationship Development: The Other Side of Trust". In McLaughlin (ed.), *Communications Yearbook 9*, Beverly Hills CA: Sage.
- McCornack, S.A., (1992) "Information Manipulation Theory," *Communication Monographs*, 59, 1-16.
- McCornack, S.A.; Levine, T.R.; Slolwczuk, K.A.; Torres, H.I.: and Campbell, D.M. (1992). "When the alteration of Information is Viewed as Deception: An Empirical Test of Information Manipulation Theory," *Communication Monographs*, 59, 1992

- McCornack, S.A.; Levine, T.R.; Morrison, K.; and Lapinski, M. (1996). "Speaking of Information Manipulation: A Critical Rejoinder," *Communication Monographs*, 63(1), 83-91.
- Miller, G.R. and Stiff, J.B. (1993). *Deceptive Communication*, Sage.
- Mohan, S. (1995). "E-mail Security Ignored: Directory Standards Exist But Enforcement Lacking," *Computerworld*, 29(39), 53-55.
- Moody, G. (1995). "Protecting Your Property from the Net Trespassers," *Computer Weekly*, Aug, 33.
- Moray D., Hiskes, D., Lee, J., and Muir, B.M. (1995) "The Psychology of Trust Between Humans and Machines," in Hoc, J.M., Cacciabue, P.C., and Hollnagel, E. (Eds.), *Expertise and Technology*, Hillsdale, NJ: Lawrence Erlbaum Associates, Publishers.
- Morrison, P.R. (1983). "A Survey of Attitudes Toward Computers," *Communications of the ACM*, 26(12), 1051-1057.
- Muir, B.M. (1987). "Trust Between Humans and Machines, and the Design of Decision Aids," *International Journal of Man-Machine Studies*, 27, 527-539.
- Muir, B.M. (1994). "Trust in Automation: Part I. Theoretical Issues in the Study of Trust and Human Intervention in Automated Systems," *Ergonomics*, 37(11), 1905-1922.
- Mungo, P. and Clough, B. (1992). *Approaching Zero*. NY: Random House.
- Munro, N. (1996). "Sketching a National Information Warfare Defense Plan," *Communications of the ACM*, 39(11), 15-17.
- O'Rielly, C. A. III, (1982). "Variations in Decision Makers' Use of Information Sources: The Impact of Quality and Accessibility of Information," *Academy of Management Journal*, 4, 756-771.
- Paradice, D.B. and Fuerst, W.L. (1991). "An MIS Data Quality Methodology Based on Optimal Error Detection," *Journal of Information Systems*, 5(1), 48-66.

- Parasuraman, R. (1984). "Sustained Attention in Detection and Discrimination," in Parasuraman and Davies (Eds.) *Varieties of Attention*. London: Academic Press Inc.
- Parasuraman, R. (1987). "Human-Computer Monitoring," *Human Factors*, 29(6), 695-706.
- Peace, D.M.S. and Easterby, R.S., (1973). "The Evaluation of User Interaction with Computer-Based Management Information Systems," *Human Factors*, 15(2), 163-177.
- Percy, T. (1986). "My Data, Right or Wrong," *Datamation*, 32(11) 123-128.
- Rempel, J.K. and Holmes, J.G. (1991). "Trust Scale," in Robinson, J.P., Shaver, P.R. and Wrightsman, L.S. (Eds.), *Measures of Personality and Social Psychological Attitudes*, New York: Academic Press, Inc.
- Ricketts, J.A. (1990). "Powers-of-Ten Information Biases," *MIS Quarterly*, 14(1), 62-77.
- Schlack, M. (1992). "IS Casts a Bigger Net," *Datamation*, 38(1), 32-34.
- Schlegel, R., (1986). "The Dark Side of the Output Candy Store," *Information Strategy: The Executives Journal*, 2(2), 37-39.
- Shimomura, T. (1996). *Takedown*. NY: Hyperion.
- Smith, G.F.; Benson, G; and Curley, S.P. (1991). "Belief, Knowledge, and Uncertainty: A Cognitive Perspective on Subjective Probabilty," *Organizational Behavior and Human Decision Process*, 48, 291-321.
- Sperling, G. (1984). "A Unified Theory of Attention and Signal Detection," in Parasuraman, R and Davies, D.R. (Eds). *Varieties of Attention*. London: Academic Press.
- Stiff, J.B., Kim, H.J. and Ramesh, C.N. (1992). "Truth Biases and Aroused Suspicion in Relational Deception," *Communications Research*, 19(3), 326-345.
- Sullivan, C.B. (1995). "Preferences for Electronic Mail in Organizational Communications Tasks," *Journal of Business Communications*, 32(1), 49-65.

- Sullivan, P. (1993). "Research Design Issues for the Study of Electronic Discussion," *Bulletin of the Association for Business Communications*, 56(2), 43-45.
- Svanks, M.I. (1988). "Integrity Analysis," *Information and Software Technology*, 30(10), 595-605.
- Tolly, K. (1994). "Business Over the Ethernet? Not Now, Not Ever," *Data Communications*, 23(7), 33-35.
- Toris, C. and DePaulo, B. (1985). "Effects of Actual Deception and Suspiciousness of Deception on Interpersonal Perceptions," *Journal of Personality and Social Psychology*, 47, 1063-1073.
- Tversky, A. and Kahneman, D. (1974). "Judgment Under Uncertainty: Heuristics and Biases," *Science*, 185, 1124-1131.
- Watson, R.T.; Kelly, G.G.; Galliers, R.D.; and Brancheau, J.C. (1997). "Key Issues in Information Systems Management: An International Perspective," *Journal of Management Information Systems*, 13(4), 91-115.
- Wiener, E.L. (1985). "Beyond the Sterile Cockpit," *Human Factors*, 27(1), 75-90.
- Wiener, E.L. (1987). "Application of Vigilance Research: Rare, Medium, or Well Done?," *Human Factors*, 29(6), 725-736.
- Wright, M.A. (1994). "Protecting Information: Effective Security Controls," *Review of Business*, 16(2) 24-29.
- Zuckerman, M., DePaulo, B.M., and Rosenthal, R., (1981) "Verbal and Nonverbal Communication of Deception" in L. Berkowitz (Ed.) *Advance in Experimental Social Psychology*. NY: Academic Press.
- Zmud, R.W. (1978). "An Emperical Investigation of the Dimensionality of Concept of Information." *Decision Sciences*, 9, 187-195.
- Zmud, R.W. (1990) "Opportunities for Strategic Information Manipulation through New Information Technology," in Fulk & Steinfield (Eds.), *Organizations and Communication Technology*, Sage.

## BIOGRAPHICAL SKETCH

Major David P. Biros (USAF) was [REDACTED]

PII Redacted

[REDACTED]. He received his Bachelor of Arts Degree in History and Secondary Education from Flagler College in St. Augustine, Florida in April of 1985. He completed a Master of Arts Degree in Public Administration for the Troy State University in June of 1990 and a Master of Science Degree in Information Resource Management from the Air Force Institute of Technology in December of 1992. He matriculated to the Florida State University in the Fall of 1995 and was conferred the degree of Doctor of Philosophy in Business Administration with a concentration in Information and Management Sciences in June 1998. Major Biros is a career Air Force officer who has completed numerous tours in the US and Europe in both the Information Management and Communications career fields. Currently, he is assigned as Assistant Professor of Information Resource Management at the Air Force Institute of Technology at Wright-Patterson Air Force Base in Fairborn, Ohio.